Cambridge studies in advanced mathematics 83

# Lectures in Logic and Set Theory

## Volume 2: Set Theory

GEORGE TOURLAKIS

CAMBRIDGE

more information - www.cambridge.org/9780521753746

This page intentionally left blank

CAMBRIDGE STUDIES IN
ADVANCED MATHEMATICS

*EDITORIAL BOARD*
B. BOLLOBAS, W. FULTON, A. KATOK, F. KIRWAN,
P. SARNAK

Lectures in Logic and Set Theory Volume 2

This two-volume work bridges the gap between introductory expositions of logic or set theory on one hand, and the research literature on the other. It can be used as a text in an advanced undergraduate or beginning graduate course in mathematics, computer science, or philosophy. The volumes are written in a user-friendly conversational lecture style that makes them equally effective for self-study or class use.

Volume 2, on formal (ZFC) set theory, incorporates a self-contained "Chapter 0" on proof techniques so that it is based on formal logic, in the style of Bourbaki. The emphasis on basic techniques will provide the reader with a solid foundation in set theory and sets a context for the presentation of advanced topics such as absoluteness, relative consistency results, two expositions of Gödel's constructible universe, numerous ways of viewing recursion, and a chapter on Cohen forcing.

George Tourlakis is Professor of Computer Science at York University of Ontario.

*Already published*

2 K. Petersen *Ergodic theory*
3 P.T. Johnstone *Stone spaces*
5 J.-P. Kahane *Some random series of functions, 2nd edition*
7 J. Lambek & P.J. Scott *Introduction to higher-order categorical logic*
8 H. Matsumura *Commutative ring theory*
10 M. Aschbacher *Finite group theory, 2nd edition*
11 J.L. Alperin *Local representation theory*
12 P. Koosis *The logarithmic integral I*
14 S.J. Patterson *An introduction to the theory of the Riemann zeta-function*
15 H.J. Baues *Algebraic homotopy*
16 V.S. Varadarajan *Introduction to harmonic analysis on semisimple Lie groups*
17 W. Dicks & M. Dunwoody *Groups acting on graphs*
19 R. Fritsch & R. Piccinini *Cellular structures in topology*
20 H. Klingen *Introductory lectures on Siegel modular forms*
21 P. Koosis *The logarithmic integral II*
22 M.J. Collins *Representations and characters of finite groups*
24 H. Kunita *Stochastic flows and stochastic differential equations*
25 P. Wojtaszczyk *Banach spaces for analysts*
26 J.E. Gilbert & M.A.M. Murray *Clifford algebras and Dirac operators in harmonic analysis*
27 A. Frohlich & M.J. Taylor *Algebraic number theory*
28 K. Goebel & W.A. Kirk *Topics in metric fixed point theory*
29 J.F. Humphreys *Reflection groups and Coxeter groups*
30 D.J. Benson *Representations and cohomology I*
31 D.J. Benson *Representations and cohomology II*
32 C. Allday & V. Puppe *Cohomological methods in transformation groups*
33 C. Soule et al. *Lectures on Arakelov geometry*
34 A. Ambrosetti & G. Prodi *A primer of nonlinear analysis*
35 J. Palis & F. Takens *Hyperbolicity, stability and chaos at homoclinic bifurcations*
37 Y. Meyer *Wavelets and operators 1*
38 C. Weibel, *An introduction to homological algebra*
39 W. Bruns & J. Herzog *Cohen-Macaulay rings*
40 V. Snaith *Explicit Brauer induction*
41 G. Laumon *Cohomology of Drinfeld modular varieties I*
42 E.B. Davies *Spectral theory and differential operators*
43 J. Diestel, H. Jarchow, & A. Tonge *Absolutely summing operators*
44 P. Mattila *Geometry of sets and measures in Euclidean spaces*
45 R. Pinsky *Positive harmonic functions and diffusion*
46 G. Tenenbaum *Introduction to analytic and probabilistic number theory*
47 C. Peskine *An algebraic introduction to complex projective geometry*
48 Y. Meyer & R. Coifman *Wavelets*
49 R. Stanley *Enumerative combinatorics I*
50 I. Porteous *Clifford algebras and the classical groups*
51 M. Audin *Spinning tops*
52 V. Jurdjevic *Geometric control theory*
53 H. Volklein *Groups as Galois groups*
54 J. Le Potier *Lectures on vector bundles*
55 D. Bump *Automorphic forms and representations*
56 G. Laumon *Cohomology of Drinfeld modular varieties II*
57 D.M. Clark & B.A. Davey *Natural dualities for the working algebraist*
58 J. McCleary *A user's guide to spectral sequences II*
59 P. Taylor *Practical foundations of mathematics*
60 M.P. Brodmann & R.Y. Sharp *Local cohomology*
61 J.D. Dixon et al. *Analytic pro-P groups*
62 R. Stanley *Enumerative combinatorics II*
63 R.M. Dudley *Uniform central limit theorems*
64 J. Jost & X. Li-Jost *Calculus of variations*
65 A.J. Berrick & M.E. Keating *An introduction to rings and modules*
66 S. Morosawa *Holomorphic dynamics*
67 A.J. Berrick & M.E. Keating *Categories and modules with K-theory in view*
68 K. Sato *Levy processes and infinitely divisible distributions*
69 H. Hida *Modular forms and Galois cohomology*
70 R. Iorio & V. Iorio *Fourier analysis and partial differential equations*
71 R. Blei *Analysis in integer and fractional dimensions*
72 F. Borceaux & G. Janelidze *Galois theories*
73 B. Bollobas *Random graphs*

# LECTURES IN LOGIC AND SET THEORY

## Volume 2: Set Theory

GEORGE TOURLAKIS

*York University*

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo

Cambridge University Press
The Edinburgh Building, Cambridge CB2 2RU, United Kingdom

Published in the United States by Cambridge University Press, New York

www.cambridge.org

Information on this title: www.cambridge.org/9780521753746

© George Tourlakis 2003

This book is in copyright. Subject to statutory exception and to the provision of relevant collective licensing agreements, no reproduction of any part may take place without the written permission of Cambridge University Press.

First published in print format 2003

ISBN-13 978-0-511-06872-0 eBook (EBL)
ISBN-10 0-511-06872-7 eBook (EBL)

ISBN-13 978-0-521-75374-6 hardback
ISBN-10 0-521-75374-0 hardback

Cambridge University Press has no responsibility for the persistence or accuracy of URLs for external or third-party internet websites referred to in this book, and does not guarantee that any content on such websites is, or will remain, accurate or appropriate.

*To the memory of my parents*

# Contents

*Preface* *page* xi

I A Bit of Logic: A User's Toolbox 1

I.1 First Order Languages 7

I.2 A Digression into the Metatheory: Informal Induction and Recursion 20

I.3 Axioms and Rules of Inference 29

I.4 Basic Metatheorems 43

I.5 Semantics 53

I.6 Defined Symbols 66

I.7 Formalizing Interpretations 77

I.8 The Incompleteness Theorems 87

I.9 Exercises 94

II The Set-Theoretic Universe, Naïvely 99

II.1 The "Real Sets" 99

II.2 A Naïve Look at Russell's Paradox 105

II.3 The Language of Axiomatic Set Theory 106

II.4 On Names 110

III The Axioms of Set Theory 114

III.1 Extensionality 114

III.2 Set Terms; Comprehension; Separation 119

III.3 The Set of All Urelements; the Empty Set 130

III.4 Class Terms and Classes 134

III.5 Axiom of Pairing 145

III.6 Axiom of Union 149

III.7 Axiom of Foundation 156

III.8 Axiom of Collection 160

III.9 Axiom of Power Set 178

III.10 Pairing Functions and Products 182
III.11 Relations and Functions 193
III.12 Exercises 210
IV The Axiom of Choice 215
IV.1 Introduction 215
IV.2 More Justification for AC; the “Constructible” Universe Viewpoint 218
IV.3 Exercises 229
V The Natural Numbers; Transitive Closure 232
V.1 The Natural Numbers 232
V.2 Algebra of Relations; Transitive Closure 253
V.3 Algebra of Functions 272
V.4 Equivalence Relations 276
V.5 Exercises 281
VI Order 284
VI.1 PO Classes, LO Classes, and WO Classes 284
VI.2 Induction and Inductive Definitions 293
VI.3 Comparing Orders 316
VI.4 Ordinals 323
VI.5 The Transfinite Sequence of Ordinals 340
VI.6 The von Neumann Universe 358
VI.7 A Pairing Function on the Ordinals 373
VI.8 Absoluteness 377
VI.9 The Constructible Universe 395
VI.10 Arithmetic on the Ordinals 410
VI.11 Exercises 426
VII Cardinality 430
VII.1 Finite vs. Infinite 431
VII.2 Enumerable Sets 442
VII.3 Diagonalization; Uncountable Sets 451
VII.4 Cardinals 457
VII.5 Arithmetic on Cardinals 470
VII.6 Cofinality; More Cardinal Arithmetic; Inaccessible Cardinals 478
VII.7 Inductively Defined Sets Revisited; Relative Consistency of GCH 494
VII.8 Exercises 512
VIII Forcing 518
VIII.1 PO Sets, Filters, and Generic Sets 520
VIII.2 Constructing Generic Extensions 524

VIII.3 Weak Forcing 528
VIII.4 Strong Forcing 532
VIII.5 Strong vs. Weak Forcing 543
VIII.6 $M[G]$ Is a CTM of ZFC If $M$ Is 544
VIII.7 Applications 549
VIII.8 Exercises 558
*Bibliography* 560
*List of Symbols* 563
*Index* 567

# Preface

This volume contains the basics of Zermelo-Fraenkel axiomatic set theory. It is situated between two opposite poles: On one hand there are elementary texts that familiarize the reader with the vocabulary of set theory and build set-theoretic tools for use in courses in analysis, topology, or algebra – but do not get into metamathematical issues. On the other hand are those texts that explore issues of current research interest, developing and applying tools (constructibility, absoluteness, forcing, etc.) that are aimed to analyze the inability of the axioms to settle certain set-theoretic questions.

Much of this volume just "does set theory", thoroughly developing the theory of ordinals and cardinals along with their arithmetic, incorporating a careful discussion of diagonalization and a thorough exposition of induction and inductive (recursive) definitions. Thus it serves well those who simply want tools to apply to other branches of mathematics or mathematical sciences in general (e.g., theoretical computer science), but also want to find out about some of the subtler results of modern set theory.

Moreover, a fair amount is included towards preparing the advanced reader to read the research literature. For example, we pay two visits to Gödel's constructible universe, the second of which concludes with a proof of the relative consistency of the axiom of choice and of the generalized continuum hypothesis with ZF. As such a program requires, I also include a thorough discussion of formal interpretations and absoluteness. The lectures conclude with a short but detailed study of Cohen forcing and a proof of the non-provability in ZF of the continuum hypothesis.

The level of exposition is designed to fit a spectrum of mathematical sophistication, from third-year undergraduate to junior graduate level (each group will find here its favourite chapters or sections that serve its interests and level of preparation).

The volume is self-contained. Whatever tools one needs from mathematical logic have been included in Chapter I. Thus, a reader equipped with a combination of sufficient mathematical maturity and patience should be able to read it and understand it. There is a trade-off: the less the maturity at hand, the more the supply of patience must be. To pinpoint this "maturity": At least two courses from among calculus, linear algebra, and discrete mathematics at the junior level should have exposed the reader to sufficient diversity of mathematical issues and proof culture to enable him or her to proceed with reasonable ease.

**A word on approach.** I use the Zermelo-Fraenkel axiom system *with* the axiom of choice (AC). This is the system known as ZFC. As many other authors do, I simplify nomenclature by allowing "proper classes" in our discussions as part of our metalanguage, but not in the formal language.

I said earlier that this volume contains the "basics". I mean this characterisation in two ways: One, that all the fundamental tools of set theory as needed elsewhere in the mathematical sciences are included in detailed exposition. Two, that I do not present any applications of set theory to other parts of mathematics, because space considerations, along with a decision to include certain advanced relative consistency results, have prohibited this.

"Basics" also entails that I do not attempt to bring the reader up to speed with respect to current research issues. However, a reader who has mastered the advanced metamathematical tools contained here will be able to read the literature on such issues.

The title of the book reflects two things: One, that all good *short* titles are taken. Two, more importantly, it advertises my conscious effort to present the material in a conversational, user-friendly lecture style. I deliberately employ classroom mannerisms (such as "pauses" and parenthetical "why"s, "what if"s, and attention-grabbing devices for passages that I feel are important). This aims at creating a friendly atmosphere for the reader, especially one who has decided to study the topic without the guidance of an instructor. Friendliness also means steering clear of the terse axiom-definition-theorem recipe, and explaining how some concepts were *arrived at* in their present form. In other words, what makes things tick. Thus, I approach the development of the key concepts of ordinals and cardinals, *initially* and *tentatively*, in the manner they were originally introduced by Georg Cantor (paradox-laden and all). Not only does this afford the reader an understanding of why the modern (von Neumann) approach is superior (and contradiction-free), but it also shows what it tries to accomplish. In the same vein, Russell's paradox is visited no less than three times, leaving us in the end with a firm understanding that it has nothing to do with the "truth" or otherwise of the much-maligned statement "$x \in x$" but it is just the result of a *diagonalization* of the type Cantor originally taught us.

**A word on coverage.** Chapter I is our "Chapter 0". It contains the tools needed to enable us do our job properly – a bit of mathematical logic, certainly no more than necessary. Chapter II informally outlines what we are about to describe axiomatically: the universe of all the "real" sets and other "objects" of our intuition, a caricature of the von Neumann "universe". It is explained that the whole fuss about axiomatic set theory[†] is to have a *formal* theory derive true statements about the von Neumann sets, thus enabling us to get to *know* the nature and structure of this universe. If this is to succeed, the chosen axioms must be seen to be "true" in the universe we are describing.

To this end I ensure via *informal discussions* that every axiom that is introduced is seen to "follow" from the principle of the formation of sets by stages, or from some similarly plausible principle devised to keep paradoxes away. In this manner the reader is constantly made aware that we are building a *meaningful* set theory that has relevance to mathematical intuition and expectations (the "real" mathematics), and is not just an artificial choice of a contradiction-free set of axioms followed by the mechanical derivation of a few theorems.

With this in mind, I even make a case for the plausibility of the axiom of choice, based on a popularization of Gödel's constructible universe argument. This occurs in Chapter IV and is informal.

The set theory we do allows *atoms* (or *Urelemente*),[‡] just like Zermelo's. The re-emergence of atoms has been defended aptly by Jon Barwise (1975) and others on technical merit, especially when one does "restricted set theories" (e.g., theory of admissible sets).

Our own motivation is not technical; rather it is philosophical and pedagogical. We find it extremely counterintuitive, especially when addressing undergraduate audiences, to tell them that all their familiar mathematical objects – the "stuff of mathematics" in Barwise's words – *are* just perverse "box-in-a-box-in-a-box . . . " formations built from an infinite supply of empty boxes. For example, should I be telling my undergraduate students that their *familiar* number "2" *really is* just a short name for something like "$\boxed{\square\,\boxed{\square}}$" ? And what will I tell them about "$\sqrt{2}$"?

[†] O.K., maybe not the *whole* fuss. Axiomatics also allow us to meaningfully ask, and attempt to answer, metamathematical questions of derivability, consistency, relative consistency, independence. But in this volume much of the fuss is indeed about learning set theory.

[‡] Allows, but does not insist that there are any.

Some mathematicians have said that set theory (without atoms) speaks only of *sets* and it chooses *not* to speak about objects such as cows or fish (colourful terms for urelements). Well, it does too! Such ("atomless") set theory is known to be perfectly capable of *constructing* "artificial" cows and fish, and can then proceed to talk about such animals as much as it pleases.

While atomless ZFC has the ability to construct or codify all the familiar mathematical objects in it, it does this so well that it betrays the prime directive of the axiomatic method, which is to have a theory that *applies* to diverse concrete (*meta* – i.e., outside the theory and in the realm of "everyday math") mathematical systems. Group theory and projective geometry, for example, fulfill the directive.

In atomless ZFC the opposite appears to be happening: One is asked to *embed* the known mathematics into the formal system.

We prefer a set theory that allows both artificial and real cows and fish, so that when we want to illustrate a point in an example utilizing, say, the everyday set of integers, $\mathbb{Z}$, we can say things like "let the atoms (be interpreted to) include the members of $\mathbb{Z}\ldots$".

But how about technical convenience? Is it not hard to include atoms in a formal set theory? In fact, not at all!

**A word on exposition devices.** I freely use a pedagogical feature that, I believe, originated in Bourbaki's books – that is, marking an important or difficult topic by placing a "winding road" sign in the margin next to it. I am using here the same symbol that Knuth employed in his TeXbook, namely, ☡, marking with it the beginning and end of an important passage.

Topics that are advanced, or of the "read at your own risk" type, *can be omitted without loss of continuity*. They are delimited by a double sign, ☡☡.

Most chapters end with several exercises. I have stopped making attempts to sort exercises between "hard" and "just about right", as such classifications are rather subjective. In the end, I'll pass on to you the advice one of my professors at the University of Toronto used to offer: "Attempt all the problems. Those you can do, don't do. Do the ones you cannot".

**What to read.** Just as in the advice above, I suggest that you read everything that you do not already know if time is no object. In a class environment the coverage will depend on class length and level, and I defer to the preferences of the instructor. I suppose that a fourth-year undergraduate audience ought to see the informal construction of the constructible universe in Chapter IV, whereas a graduate audience would rather want to see the formal version in Chapter VI. The latter group will probably also want to be exposed to Cohen forcing.

**Acknowledgments.** I wish to thank all those who taught me, a group that is too large to enumerate, in which I must acknowledge the presence and influence of my parents, my students, and the writings of Shoenfield (in particular, 1967, 1978, 1971).

The staff at Cambridge University Press provided friendly and expert support, and I thank them. I am particularly grateful for the encouragement received from Lauren Cowles and Caitlin Doggart at the initial (submission and refereeing) and advanced stages (production) of the publication cycle respectively.

I also wish to record my appreciation to Zach Dorsey of TechBooks and his team. In both volumes they tamed my English and LaTeX, fitting them to Cambridge specifications, and doing so with professionalism and flexibility.

This has been a long project that would have not been successful without the support and understanding – for my long leaves of absence in front of a computer screen – that only one's family knows how to provide.

I finally wish to thank Donald Knuth and Leslie Lamport for their typesetting systems TeX and LaTeX that make technical writing fun (and also empower authors to load the pages with ☡ and other signs).

George Tourlakis
*Toronto, March 2002*

# I

# A Bit of Logic: A User's Toolbox

This prerequisite chapter – what some authors call a "Chapter 0" – is an abridged version of Chapter I of volume 1 of my *Lectures in Logic and Set Theory*. It is offered here just in case that volume *Mathematical Logic* is not readily accessible.

Simply put, logic[†] is about *proofs* or *deductions*. From the point of view of the *user* of the subject – whose best interests we attempt to serve in this chapter – logic ought to be just a toolbox which one can employ to prove theorems, for example, in set theory, algebra, topology, theoretical computer science, etc.

The volume at hand is about an important specimen of a mathematical theory, or logical theory, namely, axiomatic set theory. Another significant example, which we do not study here, is arithmetic. Roughly speaking, a mathematical theory consists on one hand of assumptions that are specific to the subject matter – the so-called *axioms* – and on the other hand a toolbox of logical rules. One usually performs either of the following two activities with a mathematical theory: One may choose to work *within the theory*, that is, employ the tools and the axioms for the sole purpose of proving theorems. Or one can take the entire theory as an *object of study* and study it "from the outside" as it were, in order to pose and attempt to answer questions about the power of the theory (e.g., "does the theory have as theorems all the 'true' statements about the subject matter?"), its reliability (meaning whether it is free from contradictions or not), how its reliability is affected if you add new assumptions (axioms), etc.

Our development of set theory will involve both types of investigations indicated above:

(1) Primarily, we will act as *users* of logic in order to deduce "true" statements about sets (i.e., theorems of set theory) as consequences of certain

[†] We drop the qualifier "mathematical" from now on, as this is the only type of logic we are about.

"obviously true"[†] statements that we accept up front without proof, namely, the ZFC axioms.[‡] This is pretty much analogous to the behaviour of a geometer whose job is to prove theorems of, say, Euclidean geometry.

(2) We will also look at ZFC from the outside and address some issues of the type "is such and such a sentence (of set theory) provable from the axioms of ZFC and the rules of logic alone?"

It is evident that we need a *precise formulation* of set theory, that is, we must turn it into a *mathematical object* in order to make task (2), above, a meaningful mathematical activity.[§] This dictates that we develop logic itself *formally*, and subsequently set theory as a *formal theory*.

Formalism,[¶] roughly speaking, is the *abstraction* of the reasoning processes (proofs) achieved by deleting any references to the "truth content" of the component mathematical statements (formulas). What is important in formalist reasoning is solely the syntactic *form* of (mathematical) statements as well as that of the proofs (or deductions) within which these statements appear.

A formalist builds an *artificial language*, that is, an infinite – but *finitely specifiable*[#] – collection of "words" (meaning *symbol sequences*, also called *expressions*). He[||] then uses this language in order to build deductions – that is, *finite sequences* of words – in such a manner that, at each step, he writes down a word if and only if it is "certified" to be *syntactically correct* to do so. "Certification" is granted by a toolbox consisting of the very same rules of logic that we will present in this chapter.

The formalist may pretend, if he so chooses, that the words that appear in a proof are meaningless sequences of meaningless symbols. Nevertheless, such posturing cannot hide the fact that (in any purposefully designed theory) these

[†] We often quote a word or cluster of related words as a warning that the crude English meaning is not necessarily the intended meaning, or it may be ambiguous. For example, the first "true" in the sentence where this footnote originates is technical, but in a *first approximation* may be taken to mean what "true" means in English. "Obviously true" is an ambiguous term. Obvious to whom? However, the point is – to introduce another ambiguity – that "reasonable people" will accept the truth of the (ZFC) axioms.

[‡] This is an acronym reflecting the names of *Zermelo* and *Fraenkel* – the founders of this particular axiomatization – and the fact that the so-called axiom of *choice* is included.

[§] Here is an analogy: It is the precision of the rules for the game of chess that makes the notion of analyzing a chessboard configuration meaningful.

[¶] The person who practises formalism is a formalist.

[#] The finite specification is achieved by a finite collection of "rules", repeated applications of which build the words.

[||] *By definition*, "he", "his", "him" – and their derivatives – are gender-neutral in this volume.

words *codify* "true" (intuitively speaking) statements. Put bluntly, we must have something meaningful to talk about before we bother to codify it.

Therefore, a formal theory is a laboratory version (artificial replica or *simulation*, if you will) of a "real" mathematical theory of the type encountered in mathematics,[†] and formal proofs do unravel (codified versions of) "truths" beyond those embodied in the adopted axioms.

It will be reassuring for the uninitiated that it is a fact of logic that the totality of the "universally true" statements – that is, those that hold in all of mathematics and not only in specific theories – coincides with the totality of statements that we can *deduce purely formally* from some simple universally true *assumptions* such as $x = x$, without any reference to meaning or "truth" (Gödel's completeness theorem for first order logic). In short, in this case formal deducibility is as powerful as "truth". The flip side is that formal deducibility *cannot* be as powerful as "truth" when it is applied to *specific* mathematical theories such as set theory or arithmetic (Gödel's incompleteness theorem).

Formalization allows us to understand the deeper reasons that have prevented set theorists from settling important questions such as the *continuum hypothesis* – that is, the statement that there are no cardinalities between that of the set of natural numbers and that of the set of the reals. This understanding is gathered by "running diagnostics" on our laboratory replica of set theory. That is, just as an engineer evaluates a new airplane design by building and testing a model of the real thing, we can find out, with some startling successes, what are the limitations of our theory, that is, what our assumptions are incapable of logically implying.[‡] If the replica is well built,[§] we can then learn something about the behaviour of the real thing.

In the case of formal set theory and, for example, the question of our failure to resolve the continuum hypothesis, such diagnostics (the methods of Gödel and Cohen – see Chapters VI and VIII) return a simple answer: We have not included enough assumptions in (whether "real" or "formal") set theory to settle this question one way or another.

[†] Examples of "real" (non-formalized) theories are Euclid's geometry, topology, the theory of groups, and, of course, Cantor's "naïve" or "informal" set theory.

[‡] In model theory "model" means exactly the opposite of what it means here. A model airplane abstracts the real thing. A model of a formal (i.e., abstract) theory is a "concrete" or "real" version of the abstract theory.

[§] This is where it pays to choose reasonable assumptions, assumptions that are "obviously true".

But what about the interests of the reader who only wants to *practise* set theory, and who therefore may choose to skip the parts of this volume that just *talk about* set theory? Does, perchance, formalism put him into an unnecessary straitjacket?

We think not. Actually it is easier, and safer, to reason formally than to do so informally. The latter mode often mixes syntax and semantics (meaning), and there is always the danger that the "user" may assign incorrect (i.e., convenient, but not general) meanings to the symbols that he manipulates, a phenomenon that anyone who is teaching mathematics must have observed several times with some distress.

Another uncertainty one may encounter in an informal approach is this: "What can we allow to be a 'property' in mathematics?" This is an important question, for we often want to collect objects that share a common property, or we want to prove some property of the natural numbers by induction or by the least principle. But what *is* a property? Is colour a property? How about mood? It is not enough to say, "no, these are not properties", for these are just *two* frivolous examples. The question is how to describe accurately and unambiguously the *infinite variety* of properties that *are* allowed. Formalism can do just that.[†]

"Formalism for the user" is not a revolutionary slogan. It was advocated by Hilbert, the founder of formalism, partly as a means of – as he believed[‡] – formulating mathematical theories in a manner that allows one to check them (i.e., run diagnostic tests on them) for freedom from contradiction,[§] but also as the *right way* to do mathematics. By this proposal he hoped to salvage mathematics itself – which, Hilbert felt, was about to be destroyed by the Brouwer school of intuitionist thought. In a way, his program could bridge the gap between the classical and the intuitionist camps, and there is some evidence that Heyting (an influential intuitionist and contemporary of Hilbert) thought that such a *rapprochement* was possible. After all, since meaning is irrelevant to a formalist, all that he is doing (in a proof) is shuffling finite sequences of

[†] Well, almost. So-called cardinality considerations make it impossible to describe *all* "good" properties formally. But, practically and empirically speaking, we can define all that matter for "doing mathematics".

[‡] This belief was unfounded, as Gödel's incompleteness theorems showed.

[§] Hilbert's *metatheory* – that is, the "world" or "lab" outside the theory, where the replica is actually manufactured – was *finitary*. Thus – Hilbert believed – all this theory building and theory checking ought to be effected by finitary means. This was another ingredient that was consistent with peaceful coexistence with the intuitionists. And, alas, this ingredient was the one that – as some writers put it – destroyed Hilbert's program to found mathematics on his version of formalism. Gödel's incompleteness theorems showed that a finitary metatheory is not up to the task.

symbols, never having to handle or argue about infinite objects – a good thing, as far as an intuitionist is concerned.[†]

In support of the "formalism for the user" position we must not fail to mention Bourbaki's (1966a) monumental work, which is a formalization of a huge chunk of mathematics, including set theory, algebra, topology, and theory of integration. This work is strictly for the *user* of mathematics, not for the *metamathematician* who *studies* formal theories. Yet, it is fully formalized, true to the spirit of Hilbert, and it comes in a self-contained package, including a "Chapter 0" on formal logic.

More recently, the proposition of employing formal reasoning as a tool has been gaining support in a number of computer science undergraduate curricula, where logic and discrete mathematics are taught in a formalized setting, starting with a rigorous course in the two logical calculi (propositional and predicate), emphasizing the point of view of the user of logic (and mathematics) – hence with an attendant emphasis on *calculating* (i.e., writing and annotating formal) proofs. Pioneering works in this domain are the undergraduate text (1994) and the paper (1995) of Gries and Schneider.

You are urged to master the technique of writing formal proofs by studying how we go about it throughout this volume, especially in Chapter III.[‡] You will find that writing and annotating formal proofs is a discipline very much like computer programming, so it cannot be that hard. Computer programming is taught in the first year, isn't it?[§]

[†] True, a formalist applies classical logic, while an intuitionist applies a different logic where, for example, double negation is not removable. Yet, unlike a Platonist, a formalist does not believe – or he does not have to disclose to his intuitionist friends that he might do – that infinite sets exist *in the metatheory*, as his tools are just finite symbol sequences. To appreciate the tension here, consider this anecdote: It is said that when Kronecker – the father of intuitionism – was informed of Lindemann's proof (1882) that $\pi$ is transcendental, while he granted that this was an interesting result, he also dismissed it, suggesting that $\pi$ – whose decimal expansion is, of course, infinite but not periodic – "does not exist" (see Wilder (1963, p. 193)). We do not propound the tenets of intuitionism here, but it is fair to state that infinite sets *are* possible in intuitionistic mathematics as this has later evolved in the hands of Brouwer and his Amsterdam school. However, such sets must be (like all sets of intuitionistic mathematics) *finitely generated* – just like our formal languages and the set of theorems (the latter provided that our axioms are too) – in a sense that may be familiar to some readers who have had a course in automata and language theory. See Wilder (1963, p. 234).

[‡] Many additional paradigms of formal proofs, in the context of arithmetic, are found in Chapter II of volume 1 of these *Lectures*.

[§] One must not gather the impression that formal proofs are just obscure sequences of symbol sequences akin to Morse code. Just as one does in computer programming, one also uses *comments* in formal proofs – that is, annotations (in English, Greek, or your favourite natural language) that aim to explain or justify for the benefit of the reader the various proof steps. At some point, when familiarity allows and the length of (formal) proofs becomes prohibitive, we agree to relax the proof style. Read on!

It is also fair to admit, in defense of "semantic reasoning", that meaning is an important tool for formulating conjectures, for analyzing a given proof in order to figure out what makes it tick, or indeed for *discovering* the proof, in rough outline, in the first place. For these very reasons we supplement many of our formal arguments in this volume with discussions that are based on intuitive semantics, and with several examples taken from informal mathematics.

We forewarn the reader of the inevitability with which the *informal* language of sets already intrudes in this chapter (as it indeed does in all mathematics). More importantly, some of the elementary results of Cantorian naïve set theory are needed here. Conversely, *formal* set theory needs the tools and some of the results developed here. This apparent "chicken or egg" phenomenon is often called "bootstrapping",[†] not to be confused with "circularity" – which it is not: Only informal set theory notation and results are needed here in order to found *formal* set theory.

This is a good place to summarize our grand plan:

First (in this chapter), we will formalize the rules of reasoning in general – as these apply to all mathematics – and develop their properties. We will skip the detailed study of the interaction between formalized rules and their *intended meaning* (semantics), as well as the study of the limitations of these formalized rules. Nevertheless, we will state without proof the relevant important results that come into play here, the *completeness* and *incompleteness* theorems (both due to Kurt Gödel).

Secondly (starting with the next chapter), once we have learnt *about* these tools of formalized reasoning – what they are and how to use them – we will next become *users* of formal logic so that we can discover important theorems of (or, as we say, develop) set theory. Of course, we will not forget to run a few diagnostics. For example, Chapter VIII is entirely on metamathematical issues.

Formal theories, and their artificial languages, are defined (built) and "tested" *within* informal mathematics (the latter also called "real" mathematics by Platonists). The first theory that we build here is general-purpose, or "pure", formal logic. We can then build mathematical *formal theories* (e.g., set theory) by just adding "impurities", namely, the appropriate special symbols and appropriate special assumptions (written in the artificial formal language).

We *describe* precisely how we construct these languages and theories using the usual abundance of mathematical notation, notions, and techniques available

[†] The term "bootstrapping" is suggestive of a person pulling himself up by his bootstraps. Reputedly, this technique, which is pervasive, among others, in the computer programming field – as alluded to in the term "booting" – was invented by Baron Münchhausen.

to us, augmented by the descriptive power of natural language (e.g., English, or Greek, or French, or German, or Russian), as particular circumstances or geography might dictate. This *milieu* within which we build, pursue, and study our theories – besides "real mathematics" – is also often called the *metatheory*, or more generally, *metamathematics*. The language we speak while at it, this *mélange* of mathematics and natural language, is the *metalanguage*.

## I.1. First Order Languages

In the most abstract and thus simplest manner of describing it, a *formalized mathematical theory* (also, *formalized logical theory*) consists of the following sets of things: a set of basic or primitive symbols, $\mathscr{V}$, used to build *symbol sequences* (also called strings, or expressions, or words, *over* $\mathscr{V}$); a set of strings, **Wff**, over $\mathscr{V}$, called the *formulas* of the theory; and finally, a *subset* of **Wff**, **Thm**, the set of *theorems* of the theory.[†]

Well, this is the *extension* of a theory, that is, the explicit set of objects in it. How is a theory *given*?

In most cases of interest to the mathematician it is given by specifying $\mathscr{V}$ and two sets of simple rules, namely, formula-building rules and theorem-building rules. Rules from the first set allow us to build, or *generate*, **Wff** from $\mathscr{V}$. The rules of the second set generate **Thm** from **Wff**. In short (e.g., Bourbaki (1966b)), *a theory consists of an alphabet of primitive symbols and* rules *used to generate the "language of the theory" (meaning, essentially,* **Wff***) from these symbols, and some additional rules used to generate the theorems.* We expand on this below.

**I.1.1 Remark.** What is a rule? We run the danger of becoming circular or too pedantic if we overdefine this notion. Intuitively, the rules we have in mind are string manipulation rules – that is, "black boxes" (or functions) that receive string inputs and respond with string outputs. For example, a well-known theorem-building rule receives as input a formula and a variable, and it returns (essentially) the string composed of the symbol $\forall$, immediately followed by the variable and, in turn, immediately followed by the formula.[‡] □

(1) First off, the (*first order*) *formal language*, $L$, where the theory is "spoken"[§] is a triple ($\mathscr{V}$, **Term**, **Wff**), that is, it has three important components, each of them a set. $\mathscr{V}$ is the *alphabet* (or vocabulary) of the language. It is the

[†] For a less abstract, but more detailed view of theories see p. 39.

[‡] This rule is usually called "generalization".

[§] We will soon say what makes a language "first order".

collection of the *basic* syntactic "bricks" (symbols) that we use to form symbol sequences (or *expressions*) that are *terms* (members of **Term**) or *formulas* (members of **Wff**). We will ensure that the processes that build terms or formulas, using the basic building blocks in $\mathscr{V}$, are (intuitively) *algorithmic* ("mechanical"). Terms will formally codify objects, while formulas will formally codify statements about objects.

(2) *Reasoning* in the theory will be the process of discovering "true statements" about objects – that is, *theorems*. This discovery journey begins with certain formulas which codify statements that we take for granted (i.e., accept without proof as "basic truths"). Such formulas are the *axioms*. There are two types of axioms. *Special*, or *nonlogical*, axioms are to describe specific aspects of any theory that we might be building; they are "basic truths" in a restricted context. For example, "$x + 1 \neq 0$" is a special axiom that contributes towards the characterization of number theory over $\mathbb{N}$. This is a "basic truth" in the context of $\mathbb{N}$ but is certainly not true of the integers or the rationals – which is good, because we do not want to confuse $\mathbb{N}$ with the integers or the rationals. The other kind of axiom will be found in *all* theories. It is the kind that is "universally valid", that is, *not* a theory-specific truth but one that holds in all branches of mathematics (for example, "$x = x$" is such a universal truth). This is why this type of axiom will be called *logical*.

(3) Finally, we will need *rules* for reasoning, actually called *rules of inference*. These are rules that allow us to deduce, or derive, a true statement from other statements that we have already established as being true.[†] These rules will be chosen to be oblivious to meaning, being only conscious of *form*. They will apply to statement configurations of certain *recognizable forms* and will produce (derive) new statements of some corresponding recognizable forms (see Remark I.1.1).

**I.1.2 Remark.** We may think of axioms (of either logical or nonlogical type) as being special cases of rules, that is, rules that receive *no* input in order to produce an output. In this manner item (2) above is subsumed by item (3), thus we are faithful to our abstract definition of theory (where axioms were not mentioned).

An example, outside mathematics, of an inputless rule is the rule invoked when you type **date** on your computer keyboard. This rule receives no input, and outputs the current date on your screen. □

We next look carefully into (first order) formal languages.

[†] The generous use of the term "true" here is only meant to motivate. "Provable" or "deducible" formula, or "theorem", will be the technically precise terminology that we will soon define to replace the term "true statement".

There are two parts in each first order alphabet. The first, the collection of the *logical symbols*, is common to all first order languages (regardless of which theory is spoken in them). We describe this part immediately below.

**Logical Symbols.**

**LS.1.** *Object or individual variables*. An *object variable* is any one symbol out of the unending sequence $v_0, v_1, v_2, \ldots$. In practice – whether we are using logic as a tool or as an object of study – we agree to be sloppy with notation and use, generically, $x$, $y$, $z$, $u$, $v$, $w$ with or without subscripts or primes as *names* of object variables.[†] This is just a matter of notational convenience. We allow ourselves to write, say, $z$ instead of, say, $v_{1200000000000560000009}$. Object variables (*intuitively*) "vary over" (i.e., are allowed to take *values* that are) the objects that the theory studies (e.g., numbers, sets, atoms, lines, points, etc., as the case may be).

**LS.2.** *The Boolean or propositional connectives*. These are the symbols "$\neg$" and "$\vee$".[‡] These are pronounced *not* and *or* respectively.

**LS.3.** *The existential quantifier*, that is, the symbol "$\exists$", pronounced *exists* or *for some*.

**LS.4.** *Brackets*, that is, "(" and ")".

**LS.5.** *The equality predicate*. This is the symbol "$=$", which we use to indicate that objects are "equal". It is pronounced *equals*.

The logical symbols will have a fixed interpretation. In particular, "$=$" will always be expected to mean *equals*.

The theory-specific part of the alphabet is not fixed, but varies from theory to theory. For example, in set theory we just add the nonlogical (or special) symbols, $\in$ and $U$. The first is a special *predicate symbol* (or just predicate) of *arity* 2; the second is a predicate symbol of arity 1.[§]

In number theory we adopt instead the special symbols $S$ (intended meaning: successor, or "$+\ 1$", function), $+$, $\times$, $0$, $<$, and (sometimes) a symbol for the

[†] Conventions such as this one are essentially agreements – *effected in the metatheory* – on how to be sloppy and get away with it. They are offered in the interest of user-friendliness and readability. There are also theory-specific conventions, which may allow additional names in our informal (metamathematical) notation. Such examples, in set theory, occur in the following chapters.

[‡] The quotes are *not* part of the symbol. They serve to indicate clearly, e.g., in the case of "$\vee$" here, what *is* part of the symbol and what is not (the following period is not).

[§] "arity" is derived from "ary" of "un*ary*", "bin*ary*", etc. It denotes the number of arguments needed by a symbol according to the dictates of correct syntax. Function and predicate symbols need arguments.

exponentiation operation (function) $a^b$. The first three are *function symbols* of arities 1, 2, and 2 respectively. 0 is a *constant symbol*, $<$ is a predicate of arity 2, and whatever symbol we might introduce to denote $a^b$ would have arity 2.

The following list gives the general picture.

**Nonlogical Symbols.**

**NLS.1.** A (possibly empty) set of symbols for *constants*. We normally use the metasymbols[†] $a, b, c, d, e$, with or without primes or subscripts, to stand for constants unless we have in mind some alternative "standard" formal notation in specific theories (e.g., $\emptyset$, 0, $\omega$).

**NLS.2.** A (possibly empty) set of symbols for *predicate symbols* or *relation symbols* for each possible arity $n > 0$. We normally use $P, Q, R$, generically, with or without primes or subscripts, to stand for predicate symbols. Note that $=$ is in the logical camp. Also note that theory-specific formal symbols are possible for predicates, e.g., $<, \in, U$.

**NLS.3.** Finally, a (possibly empty) set of symbols for *functions* for each possible arity $n > 0$. We normally use $f, g, h$, generically, with or without primes or subscripts, to stand for function symbols. Note that theory-specific formal symbols are possible for functions, e.g., $+, \times$.

**I.1.3 Remark.** (1) We have the option of assuming that each of the *logical* symbols that we named in **LS.1–LS.5** have no further structure and that the symbols are, ontologically, *identical to their names*, that is, they are just these exact signs drawn on paper (or on any equivalent display medium).

In this case, changing the symbols, say, $\neg$ and $\exists$ to $\sim$ and $\mathbf{E}$ respectively results in a "different" logic, but one that is, trivially, *isomorphic* to the one we are describing: Anything that we may do in, or say about, one logic trivially translates to an equivalent activity in, or utterance about, the other as long as we systematically carry out the translations of all occurrences of $\neg$ and $\exists$ to $\sim$ and $\mathbf{E}$ respectively (or vice versa).

An alternative point of view is that the symbol names are *not* the same as (identical with) the symbols they are naming. Thus, for example, "$\neg$" names the connective we pronounce **not**, by we do not know (or care) exactly what the nature of this connective is (we only care about how it behaves). Thus, the name "$\neg$" becomes just a typographical expedient and may be replaced by other names that name the same object, **not**.

This point of view gives one flexibility in, for example, deciding how the variable symbols are "implemented". It often is convenient to suppose that the

[†] *Meta*symbols are *informal* (i.e., outside the formal language) symbols that we use within "real" mathematics – the *meta*theory – in order to describe, as we are doing here, the formal language.

entire sequence of variable symbols was built from just two symbols, say, "$v$" and "|".[†] One way to do this is by saying that $v_i$ is a name for the symbol sequence

$$v\,\underbrace{|\ldots|}_{i\ |\text{'s}}\,.$$

Or, preferably – see (2) below – $v_i$ might be a name for the symbol sequence

$$v\,\underbrace{|\ldots|}_{i\ |\text{'s}}\,v.$$

Regardless of option, $v_i$ and $v_j$ will name distinct objects if $i \neq j$.

This is *not* the case for the *meta*variables (abbreviated informal names) $x, y, z, u, v, w$. *Unless we say explicitly otherwise, $x$ and $y$* may *name the same formal variable, say, $v_{131}$.*

We will mostly abuse language and deliberately confuse names with the symbols they name. For example, we will say "let $v_{1007}$ *be* an object variable . . . " rather than "let $v_{1007}$ *name* an object variable . . . ", thus *appearing* to favour option one.

(2) Any two symbols included in the alphabet are distinct. Moreover, if any of them are built from simpler sub-symbols – e.g., $v_0, v_1, v_2, \ldots$ might *really name* the strings $vv$, $v|v$, $v||v, \ldots$ – then none of them is a *substring* (or *subexpression*) of any other.[‡]

(3) A formal language, just like a natural language (such as English or Greek), is alive and evolving. The particular type of evolution we have in mind is the one effected by *formal definitions*. Such definitions continually add nonlogical symbols to the language.[§]

Thus, when we say that, e.g., "$\in$ and $U$ are the only nonlogical symbols of set theory", we are telling a small white lie. More accurately, we ought to have said that "$\in$ and $U$ are the only 'primitive' (or primeval) nonlogical symbols of set theory", for we will add loads of other symbols such as $\cup$, $\omega$, $\emptyset$, $\subset$, and $\subseteq$.

This evolution affects the (formal) language of *any* theory, not just that of set theory. □

[†] We intend these two symbols to be identical to their names. No philosophical or other purpose will be served by allowing more indirection here (such as "$v$ names $u$, which actually names $w$, which actually is . . . ").

[‡] What we have stated under (2) are *requirements*, not *metatheorems*. That is, they are nothing of the sort that we can *prove* about our formal language within everyday mathematics.

[§] This phenomenon will be visited upon in some detail in what follows. By the way, any additions are made to the *nonlogical* side of the alphabet, since all the logical symbols have been given, once and for all.

Wait a minute! If formal set theory is to serve as the foundation of all mathematics, and if the present chapter is to assist towards that purpose, then how is it that we are already employing *natural numbers* like 1200000560000009 as subscripts in the names of object variables? How is it permissible to already talk about "*sets* of symbols" when we are about to *found* a theory of sets formally? Surely we do not *have*[†] any of these items yet, do we?

This protestation is offered partly in jest. We have already said that we work within real mathematics as we build the "replicas" or "simulators" of logic and set theory. Say we are Platonists. Then the entire body of mathematics – including infinite sets, in particular the set of natural numbers $\mathbb{N}$ – is available to us as we are building whatever we are building.

We can thus describe how we *assemble* the simulator and its various parts using our knowledge of real mathematics, the language of real mathematics, and all "building blocks" available to us, including sets, infinite or otherwise, *and* natural numbers. This mathematics "exists" whether or not anyone ever builds a formal simulator for naïve set theory, or logic for that matter. Thus any apparent circularity disappears.

Now if we are *not* Platonists, then our mathematical "reality" is more restricted, but, nevertheless, building a simulator or not in *this* reality does not affect the *existence* of the reality. We will, however, this time, revise our tools. For example, if we prefer to think that *individual* natural numbers exist (up to any size), but not so their collection $\mathbb{N}$, then it is still possible to build our formal languages (in particular, as many object variables as we want) – pretty much as already described – in this restricted metatheory. We may have to be careful not to say that we have a *unending sequence* of such variables, as this would presume the existence of infinite sets *in the metatheory*.[‡] We can say instead that a variable is any object of the form $v_i$ where $i$ is a (meaningless) word of (meaningless) symbols, the latter chosen out of the set or list "0, 1, 2, 3, 4, 5, 6, 7, 8, 9".

Clearly the above approach works even within a metatheory that has failed to acknowledge the existence of *any* natural numbers.[§]

In this volume we will take the normal user-friendly position that is habitual nowadays, namely, that our metatheory is the Platonist's (infinitary) mathematics.

[†] "Do not have" in the sense of having not formally defined – or proved to exist – or both.

[‡] A finitist would have none of it, although a post-Brouwer intuitionist would be content that such a sequence is finitely describable.

[§] Hilbert, in his finitistic metatheory, *built* whatever natural numbers he needed by repeating the stroke symbol "|".

**I.1.4 Definition (Terminology about Strings).** A symbol sequence, or *expression* (or *string*), that is formed by using symbols exclusively out of a given set[†] $M$ is called *a string over the set,* or *alphabet,* $M$.

If $A$ and $B$ denote strings (say, over $M$), then the symbol $A * B$, or more simply $AB$, denotes the symbol sequence obtained by listing first the symbols of $A$ in the given left to right sequence, immediately followed by the symbols of $B$ in the given left to right sequence. We say that $AB$ *is* (more properly, *denotes* or *names*) the *concatenation* of the strings $A$ and $B$ in that order.

We denote the fact that the strings (named) $C$ and $D$ are *identical sequences* (but we just say that they are *equal*) by writing $C \equiv D$. The symbol $\not\equiv$ denotes the negation of the string equality symbol $\equiv$. Thus, if # and ? are (we do mean "are") symbols from an alphabet, then #?? $\equiv$ #?? but #? $\not\equiv$ #??. We can also employ $\equiv$ in contexts such as "let $A \equiv$ ##?", where we give the name $A$ to the string ##?.[‡]

In this book the symbol $\equiv$ will be used exclusively in the metatheory as equality of strings over some set $M$.

The symbol $\lambda$ normally denotes the *empty* string, and we postulate for it the following behaviour:

$$A \equiv A\lambda \equiv \lambda A \qquad \text{for all strings } A.$$

We say that $A$ *occurs in* $B$, or is a *substring of* $B$, iff[§] there are strings $C$ and $D$ such that $B \equiv CAD$. For example, "(" occurs four times in the (explicit) string "$\neg(()\vee)(($", at *positions* 2, 3, 7, 8. Each time this happens we have an *occurrence* of "(" in "$\neg(()\vee)(($".

If $C \equiv \lambda$, we say that $A$ is a *prefix* of $B$. If moreover $D \not\equiv \lambda$, then we say that $A$ is a *proper prefix* of $B$. □

**I.1.5 Definition (Terms).** The set of *terms*, **Term**, is the *smallest* set of strings over the alphabet $\mathscr{V}$ with the following two properties:

(1) Any of the items in **LS.1** or **NLS.1** ($x$, $y$, $z$, $a$, $b$, $c$, etc.) are included.

[†] A set that supplies symbols to be used in building strings is not special. It is just a set. However, it often has a special name: "alphabet".

[‡] Punctuation, such as ".", is not part of the string. One often avoids such footnotes by quoting strings that are explicitly written as symbol sequences. For example, if $A$ stands for the string #, one writes $A \equiv$ "#". Note that we must not write "$A$", unless we mean a string whose only symbol *is* $A$.

[§] If and only if.

(2) If $f$ is a function[†] of arity $n$ and $t_1, t_2, \ldots, t_n$ are included, then so is the string "$f t_1 t_2 \ldots t_n$".

The symbols $t$, $s$, and $u$, with or without subscripts or primes, will denote arbitrary terms. As they are used to describe the *syntax* of terms, we often call such symbols *syntactic variables* – which is synonymous with metavariables. □

☡ **I.1.6 Remark.** (1) We often abuse notation and write $f(t_1, \ldots, t_n)$ instead of $f t_1 \ldots t_n$.

(2) Definition I.1.5 is an *inductive definition*.[‡] It defines a more or less complicated term by assuming that we already know what simpler terms look like. This is a standard technique employed in real mathematics (within which we are defining the formal language). We will have the opportunity to say more about such inductive definitions – and their appropriateness – in a ☡☡ comment later on.

(3) We relate this particular manner of defining terms to our working definition of a theory (given on p. 7 immediately before Remark I.1.1 in terms of "rules" of formation). Item (2) in I.1.5 essentially says that we build new terms (from old ones) by applying the following *general rule*: Pick an arbitrary function symbol, say $f$. This has a *specific* formation rule associated with it. Namely, "for the appropriate number, $n$, of an already existing ordered list of terms, $t_1, \ldots, t_n$, build the new term consisting of $f$, immediately followed by the ordered list of the given terms".

For example, suppose we are working in the language of number theory. There is a function symbol $+$ available there. The rule associated with $+$ builds the new term $+ts$ for any prior obtained terms $t$ and $s$. Thus, $+v_1 v_{13}$ and $+v_{121} + v_1 v_{13}$ are well-formed terms. We normally write terms of number theory in *infix* notation,[§] i.e., $t+s$, $v_1+v_{13}$ and $v_{121}+(v_1+v_{13})$ (note the intrusion of brackets, to indicate sequencing in the application of $+$).

A by-product of what we have just described is that *the arity of a function symbol $f$ is whatever number of terms the associated rule will require as input.*

[†] We will omit from now on the qualification "symbol" from terminology such as "function symbol", "constant symbol", "predicate symbol".

[‡] Some mathematicians are adamant that we call this a *recursive* definition and reserve the term "induction" for "induction *proofs*". This is seen to be unwarranted hairsplitting if we consider that Bourbaki (1966b) calls *induction proofs* "*démonstrations par récurrence*". We will be less dogmatic: Either name is all right.

[§] Function symbol placed between the arguments.

(4) A crucial word used in I.1.5 (which recurs in all inductive definitions) is "smallest". It means "least inclusive" (set). For example, we may easily think of a set of strings that satisfies both conditions of the above definition, but which is *not* "smallest" by virtue of having additional elements, such as the string "¬¬(".

**Pause.** Why is "¬¬(" *not* in the smallest set as defined above, and therefore not a term?

The reader may wish to ponder further on the import of the qualification "smallest" by considering the familiar (similar) example of $\mathbb{N}$. The principle of induction in $\mathbb{N}$ ensures that this set is the *smallest* with the properties

(i) 0 is included, and
(ii) if $n$ is included, then so is $n + 1$.

By contrast, all of $\mathbb{Z}$ (set of integers), $\mathbb{Q}$ (set of rational numbers), and $\mathbb{R}$ (set of real numbers) satisfy (i) and (ii), but they are clearly *not* the "smallest" such. □

**I.1.7 Definition (Atomic Formulas).** The set of *atomic formulas*, **Af**, contains precisely:

(1) The strings $t = s$ for every possible choice of terms $t, s$.
(2) The strings $Pt_1t_2 \ldots t_n$ for every possible choices of $n$-ary predicates $P$ (for all choices of $n > 0$) and all possible choices of terms $t_1, t_2, \ldots, t_n$. □

We often abuse notation and write $P(t_1, \ldots, t_n)$ instead of $Pt_1 \ldots t_n$.

**I.1.8 Definition (Well-Formed Formulas).** The set of *well-formed formulas*, **Wff**, is the *smallest* set of strings or expressions over the alphabet $\mathscr{V}$ with the following properties:

(a) All the members of **Af** are included.
(b) If $\mathscr{A}$ and $\mathscr{B}$ denote strings (over $\mathscr{V}$) that are included, then $(\mathscr{A} \vee \mathscr{B})$ and $(\neg\mathscr{A})$ are also included.
(c) If $\mathscr{A}$ is[†] a string that is included and $x$ is *any* object variable (*which may or may not occur (as a substring) in the string* $\mathscr{A}$), then the string $((\exists x)\mathscr{A})$ is also included. We say that $\mathscr{A}$ is the *scope* of $(\exists x)$. □

[†] Denotes.

**I.1.9 Remark.**

(1) The above is yet another inductive definition. Its statement (in the metalanguage) is facilitated by the use of syntactic, or meta-, variables – $\mathscr{A}$ and $\mathscr{B}$ – used as *names* for *arbitrary* (indeterminate) formulas. We first encountered the use of syntactic variables in Definition I.1.5.

In general, we will let calligraphic capital letters $\mathscr{A}, \mathscr{B}, \mathscr{C}, \mathscr{D}, \mathscr{E}, \mathscr{F}, \mathscr{G}$ (with or without primes or subscripts) be syntactic variables (i.e., *metalinguistic* names) denoting well-formed formulas, or just *formulas*, as we often say. The definition of **Wff** given above is standard. In particular, it permits well-formed formulas such as $((\exists x)((\exists x)x = 0))$ in the interest of making the formation rules context-free.[†]

(2) The rules of syntax just given do not allow us to write things such as $\exists f$ or $\exists P$ where $f$ and $P$ are function and predicate symbols respectively. That quantification is deliberately restricted to act solely on object variables makes the language *first order*.

(3) We have already indicated in Remark I.1.6 where the arities of function and predicate symbols come from (Definitions I.1.5 and I.1.7 referred to them). These are numbers that are implicit ("hardwired") within the formation rules for terms and atomic formulas. Each function, and each predicate symbol – e.g., $+$, $\times$, $\in$, $<$ – has its own unique associated formation rule. This rule "knows" how many terms are needed (on the "input side") in order to form a term or atomic formula.

There is an alternative way of making arities of symbols known (in the *metatheory*): Rather than embedding arities in the formation rules, we can hide them inside the ontology of the symbols, not making them explicit in the name. For example, a new symbol, say $*$, can be used to record arity. That is, we can think of a predicate (or function) symbol as consisting of two parts: an arity part and an "all the rest" part, the latter needed to render the symbol unique. For example, $\in$ may be actually the *short name* for the symbol "$\in^{**}$", where this latter name is identical to the symbol it denotes, or "what you see is what you get" – see Remark I.1.3(1) and (2), p. 10. The presence of the two asterisks declares the arity. Some people say this differently: They make available to the metatheory a "function", $ar$, from "the set of all predicate and function symbols" (of a given language) to the natural numbers, so that for any function symbol $f$ or predicate symbol $P$, $ar(f)$ and $ar(P)$ yield the arity of $f$ or $P$ respectively.[‡]

[†] In some presentations, formation rule I.1.8(c) is context-sensitive: It requires that $x$ be *not* already quantified in $\mathscr{A}$.

[‡] In mathematics we understand a function as a set of input-output pairs. One can "glue" the two parts of such pairs together, as in "$\in^{**}$" – where "$\in$" is the input part and "$**$" is the output part, the latter denoting "2" – etc. Thus, the two approaches are equivalent.

(4) As a consequence of the remarks in (3) the theory can go about its job of *generating*, say, terms using the formation rules, at the same time being unable to see or discuss these arities, since these are hidden inside the rules (or inside the function or predicate names in the alternative approach). So it is *not* in the theory's "competence" to say, e.g., "hmm, this function has arity 10011132". Indeed, a theory cannot even say "hmm, so this is a function (or a term, or a wff )". A theory just generates strings. It does not test them for membership in syntactic categories, such as variable, function, term, or wff. A human user of the theory, on the other hand, can, of course, make such observations. Indeed, in theories such as set theory and arithmetic, the human user can even write a computer program that correctly makes such observations. But both of these agents, human and computer, act in the metatheory.

(5) *Abbreviations:*

**Abr1.** The string $((\forall x)\mathscr{A})$ abbreviates the string $(\neg((\exists x)(\neg\mathscr{A})))$. Thus, for any explicitly written formula $\mathscr{A}$, the former notation is informal (metamathematical), while the latter is formal (within the formal language). In particular, $\forall$ is a metalinguistic symbol. "$\forall x$" is the *universal quantifier*. $\mathscr{A}$ is its scope. The symbol $\forall$ is pronounced *for all*.

We also introduce – in the metalanguage – a number of additional Boolean connectives in order to abbreviate certain strings:

**Abr2.** *Conjunction,* $\wedge$. $(\mathscr{A} \wedge \mathscr{B})$ stands for $(\neg((\neg\mathscr{A}) \vee (\neg\mathscr{B})))$. The symbol $\wedge$ is pronounced *and*.

**Abr3.** *Classical or material implication,* $\rightarrow$. $(\mathscr{A} \rightarrow \mathscr{B})$ stands for $((\neg\mathscr{A}) \vee \mathscr{B})$. $(\mathscr{A} \rightarrow \mathscr{B})$ is pronounced *if* $\mathscr{A}$*, then* $\mathscr{B}$.

**Abr4.** *Equivalence,* $\leftrightarrow$. $(\mathscr{A} \leftrightarrow \mathscr{B})$ stands for $((\mathscr{A} \rightarrow \mathscr{B}) \wedge (\mathscr{B} \rightarrow \mathscr{A}))$.

**Abr5.** To minimize the use of brackets in the metanotation, we adopt standard *priorities* of connectives, that is, $\forall$, $\exists$, and $\neg$ have the highest; then we have (in decreasing order of priority) $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$; and we agree not to use outermost brackets. All *associativities* are *right* – that is, if we write $\mathscr{A} \rightarrow \mathscr{B} \rightarrow \mathscr{C}$, then this is a (sloppy) counterpart for $(\mathscr{A} \rightarrow (\mathscr{B} \rightarrow \mathscr{C}))$.

(6) The language just defined, $L$, is *one-sorted*, that is, it has a single *sort* or *type* of object variable. Is this not inconvenient? After all, our set theory will have both atoms and sets. In other theories, e.g., geometry, one has points, lines, and planes. One would have hoped to have different types of variables, one for each.

Actually, to do this would amount to a totally unnecessary complication of syntax. We can (and will) get away with just one sort of object variable. For example, in set theory we will also introduce a 1-ary[†] predicate, $U$, whose job is to test an object for "sethood"[‡] (vs. atom status). Similar remedies are available to other theories. For example, geometry will manage with one sort of variable, and unary predicates "Point", "Line", and "Plane".

*Apropos* language, some authors emphasize the importance of the nonlogical symbols, taking at the same time the formation rules for granted; thus they say that we have a *language*, say, "$L = \{\in, U\}$" rather than "$L = (\mathscr{V}, \mathbf{Term}, \mathbf{Wff})$ where $\mathscr{V}$ has $\in$ and $U$ as its only nonlogical symbols". That is, they use "language" for the nonlogical part of the alphabet. □ ☡

☡☡ This comment requires some familiarity with elementary concepts – such as *BNF notation* for grammar specification – encountered in a course on formal languages and automata, or, alternatively in language manuals for Algol-like programming languages (such as Algol itself, Pascal, etc.); hence the ☡☡ sign.

We have said above "This rule '*knows*' how many terms are needed (on the 'input side') in order to form a term or atomic formula." We often like to personify rules, theories, and the like, to make the exposition more relaxed. This runs the danger of being misunderstood on occasion. Here is how a rule "knows".

Syntactic definitions in the part of theoretical computer science known as *formal language theory* are given by a neat notation called BNF:[§] To fix ideas, let us say that we are describing the terms of a specific first order language that contains just one constant symbol, "$c$", and just two function symbols, "$f$" and "$g$", where we intend the former to be ternary (arity 3) and the latter of arity 5. Moreover, assume that the variables $v_0, v_1, \ldots$ are short names for $vv, v|v, \ldots$ respectively.

Then, using the *syntactic names* $\langle term \rangle$, $\langle var \rangle$, $\langle strokes \rangle$ to stand for *any* term, *any* variable, *any* string of strokes, we can recursively define these syntactic categories as follows, where we read "$\rightarrow$" as "is defined as" (the right hand side), and the big stroke, "$\Big|$" – pronounced "or" – gives *alternatives* in the

[†] More usually called *unary*.

[‡] People writing about, or teaching, set theory have made this word up. Of course, one means by it the property of being a set.

[§] Backus-Naur form. Rules (1)–(3) are in BNF. In particular the alternative symbol "$\Big|$" is part of BNF notation, and so is the $\langle \ldots \rangle$ notation for the names of syntactic categories. The "$\rightarrow$" has many typographical variants, including "::=".

definition (of the left hand side):

(1) $\langle \mathit{strokes}\rangle \to \lambda \,\Big|\, \langle \mathit{strokes}\rangle |$

(2) $\langle \mathit{var}\rangle \to v\langle \mathit{strokes}\rangle v$

(3) $\langle \mathit{term}\rangle \to c \,\Big|\, \langle \mathit{var}\rangle \,\Big|$

$$f\langle \mathit{term}\rangle\langle \mathit{term}\rangle\langle \mathit{term}\rangle \,\Big|\, g\langle \mathit{term}\rangle\langle \mathit{term}\rangle\langle \mathit{term}\rangle\langle \mathit{term}\rangle\langle \mathit{term}\rangle$$

For example, rule (1) says that a string of strokes is (defined as) either the empty string $\lambda$, or a string of strokes followed by a single stroke.

Rule (3) shows clearly how the "knowledge" of the arities of $f$ and $g$ is "hardwired" within the rule. For example, the third alternative of that rule says that a term is a string composed of the symbol "$f$" followed immediately by *three* strings, each of which is a term.

A variable that is quantified is *bound in the scope of the quantifier*. Non-quantified variables are *free*. We also give below, by induction on formulas, precise (metamathematical) definitions of "free" and "bound".

**I.1.10 Definition (Free and Bound Variables).** An object variable $x$ occurs *free* in a term $t$ or atomic formula $\mathscr{A}$ iff it occurs in $t$ or $\mathscr{A}$ as a substring (see I.1.4).

$x$ occurs free in $(\neg\mathscr{A})$ iff it occurs free in $\mathscr{A}$.

$x$ occurs free in $(\mathscr{A} \vee \mathscr{B})$ iff it occurs free in at least one of $\mathscr{A}$ and $\mathscr{B}$.

$x$ occurs free in $((\exists y)\mathscr{A})$ iff $x$ occurs free in $\mathscr{A}$ *and* $y$ is not the same variable as $x$.[†]

The $y$ in $((\exists y)\mathscr{A})$ is, of course, *not* free – even if it might be so in $\mathscr{A}$ – as we have just concluded in this inductive definition. We say that it is *bound* in $((\exists y)\mathscr{A})$. Trivially, terms and atomic formulas have no bound variables. □

**I.1.11 Remark.** (1) Of course, Definition I.1.10 takes care of the defined connectives as well, via the obvious translation procedure.

(2) *Notation.* If $\mathscr{A}$ is a formula, then we often write $\mathscr{A}[y_1, \ldots, y_k]$ to indicate interest in the variables $y_1, \ldots, y_k$, which *may or may not* be free in

[†] Recall that $x$ and $y$ are abbreviations of names such as $v_{1200098}$ and $v_{11009}$ (which name distinct variables). However, it could be that both $x$ and $y$ name $v_{101}$. Therefore it is *not* redundant to say "*and* $y$ is not the same variable as $x$". By the way, $x \not\equiv y$ says the same thing, by I.1.4.

$\mathscr{A}$. There may be other free variables in $\mathscr{A}$ that we may have chosen not to include in the list. On the other hand, if we use *round* brackets, as in $\mathscr{A}(y_1, \ldots, y_k)$, then we are implicitly asserting that $y_1, \ldots, y_k$ is the *complete list* of free variables that occur in $\mathscr{A}$. □

**I.1.12 Definition.** A term or formula is *closed* iff no free variables occur in it. A closed formula is called a *sentence*.

A formula is *open* iff it contains no quantifiers (thus, an open formula may also be closed). □

## I.2. A Digression into the Metatheory: Informal Induction and Recursion

We have already seen a number of inductive or recursive definitions in Section I.1. The reader, most probably, has already seen or used such definitions elsewhere.

We will organize the common important features of inductive definitions in this section for easy reference. We will revisit these issues, within the framework of formal set theory, in due course, but right now we need to ensure that our grasp of these notions and techniques, *at the metamathematical level*, is sufficient for our needs.

One builds a set $S$ by *recursion*, or *inductively* (or by induction), out of two ingredients: a set of *initial objects*, $\mathscr{T}$, and a set of *rules* or *operations*, $\mathscr{R}$. A member of $\mathscr{R}$ – a rule – is a (possibly infinite) *table*, or *relation*, like

| $y_1$ | $\ldots$ | $y_n$ | $z$ |
|---|---|---|---|
| $a_1$ | $\ldots$ | $a_n$ | $a_{n+1}$ |
| $b_1$ | $\ldots$ | $b_n$ | $b_{n+1}$ |
| $\vdots$ | | $\vdots$ | $\vdots$ |

If the above rule (table) is called $Q$, then we use the notations $Q(a_1, \ldots, a_n, a_{n+1})$ and[†] $\langle a_1, \ldots, a_n, a_{n+1}\rangle \in Q$ interchangeably to indicate that the *ordered sequence* or "row" $a_1, \ldots, a_n, a_{n+1}$ is present in the table. We say "$Q(a_1, \ldots, a_n, a_{n+1})$ holds" or "$Q(a_1, \ldots, a_n, a_{n+1})$ is true", but we often also say that "$Q$ applied to $a_1, \ldots, a_n$ yields $a_{n+1}$", or that "$a_{n+1}$ is a *result* or *output* of $Q$, when the latter receives *input* $a_1, \ldots, a_n$". We often abbreviate such inputs

[†] "$x \in A$" means that "$x$ is a member of – or is in – $A$" in the informal set-theoretic sense.

using *vector notation*, namely, $\vec{a}_n$ (or just $\vec{a}$, if $n$ is understood). Thus, we often write $Q(\vec{a}_{n+1})$ for $Q(a_1, \ldots, a_n, a_{n+1})$.

A rule $Q$ that has $n + 1$ columns is called $(n + 1)$-ary.

**I.2.1 Definition.** We say "a set $T$ is *closed under an* $(n + 1)$*-ary rule* $Q$" to mean that whenever $c_1, \ldots, c_n$ are all in $T$, then $d \in T$ for *all* $d$ satisfying $Q(c_1, \ldots, c_n, d)$. □

With these preliminary understandings out of the way, we now state

**I.2.2 Definition.** $S$ is *defined by recursion*, or by *induction*, from initial objects $\mathscr{I}$ and set of rules $\mathscr{R}$, provided it is the *smallest* (least inclusive) set with the properties

(1) $\mathscr{I} \subseteq S$,[†]
(2) $S$ is closed under *every* $Q$ in $\mathscr{R}$. In this case we say that $S$ is $\mathscr{R}$-closed.

We write $S = \mathrm{Cl}(\mathscr{I}, \mathscr{R})$, and say that "$S$ is the *closure of* $\mathscr{I}$ *under* $\mathscr{R}$". □

We have at once:

**I.2.3 Metatheorem (Induction on $S$).** *If* $S = \mathrm{Cl}(\mathscr{I}, \mathscr{R})$ *and if some set* $T$ *satisfies*

(1) $\mathscr{I} \subseteq T$, *and*
(2) $T$ *is closed under every* $Q$ *in* $\mathscr{R}$,

*then* $S \subseteq T$.

**Pause.** Why is the above a *meta*theorem?

The above principle of induction on $S$ is often rephrased as follows: To prove that a "property" $P(x)$ holds for all members of $\mathrm{Cl}(\mathscr{I}, \mathscr{R})$, just prove that

(a) Every member of $\mathscr{I}$ has the property, and
(b) The property *propagates* with every rule in $\mathscr{R}$, i.e., if $P(c_i)$ holds (is true) for $i = 1, \ldots, n$, and if $Q(c_1, \ldots, c_n, d)$ holds, then $d$ too has property $P(x)$ – that is, $P(d)$ holds.

[†] From our knowledge of elementary informal set theory, we recall that $A \subseteq B$ means that every member of $A$ is also a member of $B$.

Of course, this rephrased principle is valid, for if we let $T$ be the set of all objects that have property $P(x)$ – for which set one employs the well-established symbol $\{x : P(x)\}$ – then this $T$ satisfies (1) and (2) of the metatheorem.[†]

**I.2.4 Definition (Derivations and Parses).** A $(\mathscr{I}, \mathscr{R})$*-derivation*, or simply *derivation* – if $\mathscr{I}$ and $\mathscr{R}$ are understood – is a finite sequence of objects $d_1, \ldots, d_n$ $(n \geq 1)$ such that each $d_i$ is

(1) A member of $\mathscr{I}$, or[‡]
(2) For some $(r+1)$-ary $Q \in \mathscr{R}$, $Q(d_{j_1}, \ldots, d_{j_r}, d_i)$ holds, and $j_l < i$ for $l = 1, \ldots, r$.

We say that $d_i$ is *derivable within i steps.*

A derivation of an object $A$ is also called a *parse* of $a$. □

Trivially, if $d_1, \ldots, d_n$ is a derivation, then so is $d_1, \ldots, d_m$ for any $1 \leq m < n$.

If $d$ is derivable within $n$ steps, it is also derivable in $k$ steps or less for all $k > n$, since we can lengthen a derivation arbitrarily by adding $\mathscr{I}$-elements to it.

**I.2.5 Remark.** The following metatheorem shows that there is a way to "construct" $\mathrm{Cl}(\mathscr{I}, \mathscr{R})$ *iteratively*, i.e., one element at a time by repeated application of the rules.

This result shows definitively that our inductive definitions of terms (I.1.5) and well-formed formulas (I.1.8) fully conform with our working definition of theory, as an alphabet and a set of rules that are used to build formulas and theorems (p. 7). □

**I.2.6 Metatheorem.**

$$\mathrm{Cl}(\mathscr{I}, \mathscr{R}) = \{x : x\ is\ (\mathscr{I}, \mathscr{R})\text{-}derivable\ within\ some\ number\ of\ steps,\ n\}$$

*Proof.* For notational convenience let us write

$$T = \{x : x \text{ is } (\mathscr{I}, \mathscr{R})\text{-derivable within some number of steps, } n\}.$$

As we know from elementary naïve set theory, we need to show here both $\mathrm{Cl}(\mathscr{I}, \mathscr{R}) \subseteq T$ and $\mathrm{Cl}(\mathscr{I}, \mathscr{R}) \supseteq T$ to settle the claim.

$\subseteq$: We do induction on $\mathrm{Cl}(\mathscr{I}, \mathscr{R})$ (using I.2.3). Now $\mathscr{I} \subseteq T$, since every member of $\mathscr{I}$ is derivable in $n = 1$ step (why?).

[†] We are sailing too close to the wind here. It turns out that not all properties $P(x)$ lead to *sets* $\{x : P(x)\}$. Our explanation was naïve. However, formal set theory, which is meant to save us from our naïveté, upholds the principle (a)–(b) using just a slightly more complicated explanation. The reader can see this explanation in Chapter VII.

[‡] This "or" is inclusive: (1), or (2), or both.

Also, $T$ is closed under every $Q$ in $\mathscr{R}$. Indeed, let such an $(r+1)$-ary $Q$ be chosen. Let

$$Q(a_1, \ldots, a_r, b) \tag{$i$}$$

and $\{a_1, \ldots, a_r\} \subseteq T$. Thus, each $a_i$ has a $(\mathscr{I}, \mathscr{R})$-derivation. Concatenate all these derivations:

$$\ldots, a_1, \ldots, a_2, \ldots, \ldots, \ldots, a_r$$

The above is a derivation (why?). But then, so is

$$\ldots, a_1, \ldots, a_2, \ldots, \ldots, \ldots, a_r, b$$

by $(i)$. Thus, $b \in T$.

$\supseteq$: We argue this – that is, if $d \in T$, then $d \in \mathrm{Cl}(\mathscr{I}, \mathscr{R})$ – by induction on the number of steps, $n$, in which $d$ is derivable.

For $n = 1$ we have $d \in \mathscr{I}$ and we are done, since $\mathscr{I} \subseteq \mathrm{Cl}(\mathscr{I}, \mathscr{R})$.

Let us make the induction hypothesis (I.H.) that for derivations of $\le n$ steps the claim is true.

Let then $d$ be derivable within $n + 1$ steps. Thus, there is a derivation $a_1, \ldots, a_n, d$.

Now, if $d \in \mathscr{I}$, we are done as above (is this a "real case"?).

If on the other hand $Q(a_{j_1}, \ldots, a_{j_r}, d)$, then, for $i = 1, \ldots, r$, we have $a_{j_i} \in \mathrm{Cl}(\mathscr{I}, \mathscr{R})$ by the I.H.; hence $d \in \mathrm{Cl}(\mathscr{I}, \mathscr{R})$, since the closure is closed under all $Q \in \mathscr{R}$. □

**I.2.7 Example.** One can see now that $\mathbb{N} = \mathrm{Cl}(\mathscr{I}, \mathscr{R})$, where $\mathscr{I} = \{0\}$ and $\mathscr{R}$ contains just the relation $y = x + 1$ (input $x$, output $y$). Similarly, $\mathbb{Z}$, the set of all integers, is $\mathrm{Cl}(\mathscr{I}, \mathscr{R})$, where $\mathscr{I} = \{0\}$ and $\mathscr{R}$ contains just the relations $y = x + 1$ and $y = x - 1$ (input $x$, output $y$).

For the latter, the inclusion $\mathrm{Cl}(\mathscr{I}, \mathscr{R}) \subseteq \mathbb{Z}$ is trivial (by I.2.3). For $\supseteq$ we easily see that any $n \in \mathbb{Z}$ has a $(\mathscr{I}, \mathscr{R})$-derivation (and then we are done by I.2.6). For example, if $n > 0$, then $0, 1, 2, \ldots, n$ is a derivation, while if $n < 0$, then $0, -1, -2, \ldots, n$ is one. If $n = 0$, then the one-term sequence $0$ is a derivation.

Another interesting closure is obtained by $\mathscr{I} = \{3\}$ and the two relations $z = x + y$ and $z = x - y$. This is the set $\{3k : k \in \mathbb{Z}\}$ (see Exercise I.1). □

**Pause.** So, taking the first sentence of I.2.7 one step further, we note that we have just proved the induction principle for $\mathbb{N}$, for that is exactly what the "equation" $\mathbb{N} = \mathrm{Cl}(\mathscr{I}, \mathscr{R})$ says (by I.2.3). Do you agree?

There is another way to view the iterative construction of $\mathrm{Cl}(\mathscr{I}, \mathscr{R})$: The set is constructed *in stages*. Below we are using some more notation borrowed from informal set theory. For any sets $A$ and $B$ we write $A \cup B$ to indicate the set *union* which consists of all the members found in $A$ or $B$ or in both. More generally, if we have a lot of sets, $X_0, X_1, X_2, \ldots$, that is, one $X_i$ for every integer $i \geq 0$ – which we denote by the compact notation $(X_i)_{i \geq 0}$ – then we may wish to form a set that includes *all* the objects found as members all over the $X_i$, that is (using *inclusive*, or "logical", "or"s below), form

$$\{x : x \in X_0 \text{ or } x \in X_1 \text{ or } \ldots\}$$

or, more elegantly and precisely,

$$\{x : \text{for some } i \geq 0,\ x \in X_i\}$$

The latter is called the *union* of the sequence $(X_i)_{i \geq 0}$ and is often denoted by

$$\bigcup_{i \geq 0} X_i \quad \text{or} \quad \bigcup_{i \geq 0} X_i$$

Correspondingly, we write

$$\bigcup_{i \leq n} X_i \quad \text{or} \quad \bigcup_{i \leq n} X_i$$

if we only want to take a finite union, also indicated clumsily as $X_0 \cup \cdots \cup X_n$.

**I.2.8 Definition (Stages).** In connection with $\mathrm{Cl}(\mathscr{I}, \mathscr{R})$ we define the sequence of sets $(X_i)_{i \geq 0}$ by induction on $n$, as follows:

$$X_0 = \mathscr{I}$$
$$X_{n+1} = \left(\bigcup_{i \leq n} X_i\right) \cup \left\{ b : \text{ for some } Q \in \mathscr{R} \text{ and some } \vec{a}_n \text{ in} \bigcup_{i \leq n} X_i,\ Q(\vec{a}_n, b)\right\}$$

That is, to form $X_{n+1}$ we append to $\bigcup_{i \leq n} X_i$ all the outputs of all the relations in $\mathscr{R}$ acting on all possible inputs, the latter taken from $\bigcup_{i \leq n} X_i$.

We say that $X_i$ is built at *stage* $i$, from initial objects $\mathscr{I}$ and rule set $\mathscr{R}$. □

In words, at stage 0 we are given the initial objects ($X_0 = \mathscr{I}$). At stage 1 we apply all possible relations to all possible objects *that we have so far* – they form the set $X_0$ – and build the first stage set, $X_1$, by appending the outputs to what we have so far. At stage 2 we apply all possible relations to all possible objects *that we have so far* – they form the set $X_0 \cup X_1$ – and build the second stage set, $X_2$, by appending the outputs to what we have so far. And so on.

When we work in the metatheory, we take for granted that we can have simple inductive definitions on natural numbers. The reader is familiar with several such definitions, e.g.,

$$\begin{aligned} a^0 &= 1 \qquad \text{(for } a \neq 0 \text{ throughout)} \\ a^{n+1} &= a \cdot a^n \end{aligned}$$

We will (meta)prove a general theorem on the feasibility of recursive definitions later on (I.2.13).

The following theorem connects stages and closures.

**I.2.9 Metatheorem.** *With the $X_i$ as in* I.2.8*,*

$$\mathrm{Cl}(\mathscr{I}, \mathscr{R}) = \bigcup_{i \geq 0} X_i$$

*Proof.* $\subseteq$: We do induction on $\mathrm{Cl}(\mathscr{I}, \mathscr{R})$. For the basis, $\mathscr{I} = X_0 \subseteq \bigcup_{i \geq 0} X_i$.

We show that $\bigcup_{i \geq 0} X_i$ is $\mathscr{R}$-closed. Let $Q \in \mathscr{R}$ and $Q(\vec{a}_n, b)$ hold, for some $\vec{a}_n$ in $\bigcup_{i \geq 0} X_i$. Thus, by definition of union, there are integers $j_1, j_2, \ldots, j_n$ such that $a_i \in X_{j_i}$, $i = 1, \ldots, n$. If $k = \max\{j_1, \ldots, j_n\}$, then $\vec{a}_n$ is in $\bigcup_{i \leq k} X_i$; hence $b \in X_{k+1} \subseteq \bigcup_{i \geq 0} X_i$.

$\supseteq$: It suffices to prove that $X_n \subseteq \mathrm{Cl}(\mathscr{I}, \mathscr{R})$, a fact we can prove by induction on $n$. For $n = 0$ it holds by I.2.2. As an I.H. we assume the claim for all $n \leq k$.

The case for $k + 1$: $X_{k+1}$ is the union of two sets. One is $\bigcup_{i \leq k} X_i$. This is a subset of $\mathrm{Cl}(\mathscr{I}, \mathscr{R})$ by the I.H. The other is

$$\left\{ b : \text{ for some } Q \in \mathscr{R} \text{ and some } \vec{a} \text{ in } \bigcup_{i \leq k} X_i,\ Q(\vec{a}, b) \right\}$$

This too is a subset of $\mathrm{Cl}(\mathscr{I}, \mathscr{R})$, by the preceding observation and the fact that $\mathrm{Cl}(\mathscr{I}, \mathscr{R})$ is $\mathscr{R}$-closed. □

N.B. An inductively defined set can be built by stages.

**I.2.10 Definition (Immediate Predecessors; Ambiguity).** If $d \in \mathrm{Cl}(\mathscr{I}, \mathscr{R})$ and for some $Q$ and $a_1, \ldots, a_r$ it is the case that $Q(a_1, \ldots, a_r, d)$, then the $a_1, \ldots, a_r$ are *immediate $Q$-predecessors* of $d$, or just *immediate predecessors* if $Q$ is understood; for short, i.p.

A pair $(\mathscr{I}, \mathscr{R})$ is called *ambiguous* if some $d \in \mathrm{Cl}(\mathscr{I}, \mathscr{R})$ satisfies any (or all) of the following conditions:

(i) It has two (or more) distinct sets of immediate $P$-predecessors for some rule $P$.

(ii) It has both immediate $P$-predecessors *and* immediate $Q$-predecessors, for $P \neq Q$.
(iii) It is a member of $\mathscr{T}$, yet it has immediate predecessors.

If $(\mathscr{T}, \mathscr{R})$ is not ambiguous, then it is *unambiguous*. □

**I.2.11 Example.** The pair $(\{00, 0\}, \{Q\})$, where $Q(x, y, z)$ holds iff $z = xy$ (where "$xy$" denotes the concatenation of the strings $x$ and $y$, in that order), is ambiguous. For example, 0000 has the two immediate predecessor sets $\{00, 00\}$ and $\{0, 000\}$. Moreover, while 00 is an initial object, it does have immediate predecessors – namely, the set $\{0, 0\}$ (or, what amounts to the same thing, $\{0\}$). □

**I.2.12 Example.** The pair $(\mathscr{T}, \mathscr{R})$ where $\mathscr{T} = \{3\}$ and $\mathscr{R}$ consists of $z = x + y$ and $z = x - y$ is ambiguous. Even 3 has (infinitely many) distinct sets of i.p. (e.g., any $\{a, b\}$ such that $a + b = 3$, or $a - b = 3$).

The pairs that effect the definition of **Term** (I.1.5) and **Wff** (I.1.8) are unambiguous (see Exercises I.2 and I.3). □

**I.2.13 Metatheorem (Definition by Recursion).** *Let $(\mathscr{T}, \mathscr{R})$ be unambiguous, and* $\mathrm{Cl}(\mathscr{T}, \mathscr{R}) \subseteq A$*, where $A$ is some set. Let also $Y$ be a set, and*[†] $h : \mathscr{T} \to Y$ *and $g_Q$, for each $Q \in \mathscr{R}$, be given functions. For any $(r+1)$-ary $Q$, an input for the function $g_Q$ is a sequence $\langle a, b_1, \ldots, b_r\rangle$, where $a$ is in $A$ and the $b_1, \ldots, b_r$ are all in $Y$. All the $g_Q$ yield outputs in $Y$.*

*Under these assumptions, there is a* unique *function* $f : \mathrm{Cl}(\mathscr{T}, \mathscr{R}) \to Y$ *such that*

$$y = f(x) \quad \textit{iff} \quad \begin{cases} y = h(x) & \textit{and } x \in \mathscr{T} \\ \quad \textit{or, for some } Q \in \mathscr{R}, & \\ y = g_Q(x, o_1, \ldots, o_r) & \textit{and } Q(a_1, \ldots, a_r, x) \textit{ holds,} \\ \quad \textit{where } o_i = f(a_i) \textit{ for } i = 1, \ldots, r & \end{cases} \tag{1}$$

The reader may wish to skip the proof on first reading.

*Proof. Existence part.* For each $(r + 1)$-ary $Q \in \mathscr{R}$, define $\widehat{Q}$ by[‡]

$$\widehat{Q}\big(\langle a_1, o_1\rangle, \ldots, \langle a_r, o_r\rangle, \langle b, g_Q(b, o_1, \ldots, o_r)\rangle\big) \text{ iff } Q(a_1, \ldots, a_r, b) \tag{2}$$

[†] The notation $f : A \to B$ is common in informal (and formal) mathematics. It denotes a function $f$ that receives "inputs" from the set $A$ and yields "outputs" in the set $B$.

[‡] For a relation $Q$, writing just "$Q(a_1, \ldots, a_r, b)$" is equivalent to writing "$Q(a_1, \ldots, a_r, b)$ holds".

For any $a_1, \ldots, a_r, b$, the above definition of $\widehat{Q}$ is effected for all possible choices of $o_1, \ldots, o_r$ such that $g_Q(b, o_1, \ldots, o_r)$ is defined.

Collect now all the $\widehat{Q}$ to form a set of rules $\widehat{\mathscr{R}}$.

Let also $\widehat{\mathscr{T}} = \{\langle x, h(x)\rangle : x \in \mathscr{T}\}$.

We will verify that the set $F = \mathrm{Cl}(\widehat{\mathscr{T}}, \widehat{\mathscr{R}})$ is a 2-ary relation that for every input yields *at most one* output, and therefore is a function. For such a relation it is customary to write, letting the context fend off the obvious ambiguity in the use of the letter $F$,

$$y = F(x) \quad \text{iff} \quad F(x, y) \tag{$*$}$$

We will further verify that replacing $f$ in (1) above by $F$ results in a valid equivalence (the "iff" holds). That is, $F$ satisfies (1).

**(a)** We establish that $F$ is a relation composed of pairs $\langle x, y\rangle$ ($x$ is input, $y$ is output) where $x \in \mathrm{Cl}(\mathscr{T}, \mathscr{R})$ and $y \in Y$. This follows easily by induction on $F$ (I.2.3), since $\widehat{\mathscr{T}} \subseteq F$, and the property (of containing such pairs) propagates with each $\widehat{Q}$ (recall that the $g_Q$ yield outputs in $Y$).

**(b)** We next show "if $\langle x, y\rangle \in F$ and $\langle x, z\rangle \in F$, then $y = z$" – that is, $F$ is single-valued, or well defined, in short, it is a *function*. We again employ induction on $F$, thinking of the quoted statement as a "property" of the pair $\langle x, y\rangle$: Suppose that $\langle x, y\rangle \in \widehat{\mathscr{T}}$ and let also $\langle x, z\rangle \in F$. By I.2.6, $\langle x, z\rangle \in \widehat{\mathscr{T}}$, *or* $\widehat{Q}(\langle a_1, o_1\rangle, \ldots, \langle a_r, o_r\rangle, \langle x, z\rangle)$, where $Q(a_1, \ldots, a_r, x)$ and $z = g_Q(x, o_1, \ldots, o_r)$, for some $(r+1)$-ary $\widehat{Q}$ and $\langle a_1, o_1\rangle, \ldots, \langle a_r, o_r\rangle$ in $F$. The right hand side of the italicized "or" cannot hold for an unambiguous $(\mathscr{T}, \mathscr{R})$, since $x$ cannot have i.p. Thus $\langle x, z\rangle \in \widehat{\mathscr{T}}$, hence $y = h(x) = z$. To prove that the property propagates with each $\widehat{Q}$, let

$$\widehat{Q}(\langle a_1, o_1\rangle, \ldots, \langle a_r, o_r\rangle, \langle x, y\rangle)$$

but also

$$\widehat{P}(\langle b_1, o'_1\rangle, \ldots, \langle b_l, o'_l\rangle, \langle x, z\rangle)$$

where $Q(a_1, \ldots, a_r, x)$, $P(b_1, \ldots, b_l, x)$, and

$$y = g_Q(x, o_1, \ldots, o_r) \quad \text{and} \quad z = g_P(x, o'_1, \ldots, o'_l) \tag{3}$$

Since $(\mathscr{T}, \mathscr{R})$ is unambiguous, $Q = P$ (hence also $\widehat{Q} = \widehat{P}$), $r = l$, and $a_i = b_i$, for $i = 1, \ldots, r$. By the I.H., $o_i = o'_i$, for $i = 1, \ldots, r$; hence $y = z$ by (3).

**(c)** Finally, we show that $F$ satisfies (1). We do induction on $\mathrm{Cl}(\widehat{\mathscr{I}}, \widehat{\mathscr{R}})$, to prove $\leftarrow$: If $x \in \mathscr{I}$ and $y = h(x)$, then $F(x, y)$ (i.e., $y = F(x)$ in the alternative notation $(*)$), since $\widehat{\mathscr{I}} \subseteq F$. Let next $y = g_Q(x, o_1, \ldots, o_r)$ and $Q(a_1, \ldots, a_r, x)$, where also $F(a_i, o_i)$, for $i = 1, \ldots, r$. By (2), $\widehat{Q}\big(\langle a_1, o_1\rangle, \ldots, \langle a_r, o_r\rangle, \langle x, g_Q(x, o_1, \ldots, o_r)\rangle\big)$; thus – $F$ being closed under all the rules in $\widehat{R}$ – $F(x, g_Q(b, o_1, \ldots, o_r))$ holds, in short, $F(x, y)$ or $y = F(x)$. For $\rightarrow$, now we assume that $F(x, y)$ holds and we want to infer the right hand side (of *iff*) in (1). We employ Metatheorem I.2.6.

*Case 1.* Let $\langle x, y\rangle$ be $F$-derivable[†] in $n = 1$ step. Then $\langle x, y\rangle \in \widehat{\mathscr{I}}$. Thus $y = h(x)$.

*Case 2.* Suppose next that $\langle x, y\rangle$ is $F$-derivable within $n + 1$ steps, namely, we have a derivation

$$\langle x_1, y_1\rangle, \langle x_2, y_2\rangle, \ldots, \langle x_n, y_n\rangle, \langle x, y\rangle \tag{4}$$

where $\widehat{Q}(\langle a_1, o_1\rangle, \ldots, \langle a_r, o_r\rangle, \langle x, y\rangle)$ and $Q(a_1, \ldots, a_r, x)$ (see (2)), and each of $\langle a_1, o_1\rangle, \ldots, \langle a_r, o_r\rangle$ appears in the above derivation, to the left of $\langle x, y\rangle$. This entails (by (2)) that $y = g_Q(x, o_1, \ldots, o_r)$. Since the $\langle a_i, o_i\rangle$ appear in (4), $F(a_i, o_i)$ holds for $i = 1, \ldots, r$. Thus, $\langle x, y\rangle$ satisfies the right hand side of *iff* in (1), once more.

*Uniqueness part.* Let the function $K$ also satisfy (1). We show, by induction on $\mathrm{Cl}(\mathscr{I}, \mathscr{R})$, that

$$\text{for all } x \in \mathrm{Cl}(\mathscr{I}, \mathscr{R}) \text{ and all } y \in Y, \qquad y = F(x) \text{ iff } y = K(x) \tag{5}$$

$\rightarrow$: Let $x \in \mathscr{I}$, and $y = F(x)$. By lack of ambiguity, the case conditions of (1) are mutually exclusive. Thus, it must be that $y = h(x)$. But then, $y = K(x)$ as well, since $K$ satisfies (1) too.

Let now $Q(a_1, \ldots, a_r, x)$ and $y = F(x)$. By (1), there are (unique, as we now know) $o_1, \ldots, o_r$ such that $o_i = F(a_i)$ for $i = 1, \ldots, r$, and $y = g_Q(x, o_1, \ldots, o_r)$. By the I.H., $o_i = K(a_i)$. But then (1) yields $y = K(x)$ as well (since $K$ satisfies (1)).

$\leftarrow$: Just interchange the letters $F$ and $K$ in the above argument. □

The above clearly is valid for functions $h$ and $g_Q$ that may fail to be defined everywhere in their "natural" input sets. To be able to have this degree of generality without having to state additional definitions (such as those of *left fields*, *right fields*, *partial functions*, *total functions*, *nontotal functions*, and Kleene *weak equality*) we have stated the recurrence (1) the way we did (to

[†] $\mathrm{Cl}(\widehat{\mathscr{I}}, \widehat{\mathscr{R}})$-derivable.

keep an eye on both the input and output side of things) rather than the usual

$$f(x) = \begin{cases} h(x) & \text{if } x \in \mathscr{I} \\ g_Q(x, f(a_1), \ldots, f(a_r)) & \text{if } Q(a_1, \ldots, a_r, x) \text{ holds,} \end{cases}$$

Of course, if all the $g_Q$ and $h$ are defined everywhere on their input sets (i.e., they are "total"), then $f$ is defined everywhere on $\mathrm{Cl}(\mathscr{I}, \mathscr{R})$ (see Exercise I.4). ☡☡

## I.3. Axioms and Rules of Inference

Now that we have our language $L$, we will embark on using it to formally effect deductions. These deductions start at the axioms. Deductions employ "acceptable", purely syntactic – i.e., based on form, not on substance – rules that allow us to write a formula down (to deduce it) solely because certain other formulas *that are syntactically related to it* were already deduced (i.e., already written down). These string-manipulation rules are called *rules of inference*. We describe in this section the axioms and the rules of inference that we will accept into our logical calculus and that are common to all theories.

We start with a precise definition of *tautologies* in our first order language $L$.

**I.3.1 Definition (Prime Formulas in Wff. Propositional Variables).** A formula $\mathscr{A} \in$ **Wff** is a *prime formula* or a *propositional variable* iff it is either

**Pri1.** atomic or
**Pri2.** a formula of the form $((\exists x)\mathscr{A})$.

We use the lowercase letters $p, q, r$ (with or without subscripts or primes) to denote arbitrary prime formulas (propositional variables) of our language. □

☡ That is, a prime formula either has no propositional connectives, or if it does, it hides them inside the scope of $(\exists x)$.

We may think of a propositional variable as a "blob of ink" that is all that a myopic being makes out of a formula described in I.3.1. The same being will see an arbitrary well-formed formula as a bunch of blobs, brackets and Boolean connectives $(\neg, \vee)$, "correctly connected" as stipulated below.[†] ☡

**I.3.2 Definition (Propositional Formulas).** The set of propositional formulas over $\mathscr{V}$, denoted here by **Prop**, is the smallest set such that:

(1) Every propositional variable (over $\mathscr{V}$) is in **Prop**.
(2) If $\mathscr{A}$ and $\mathscr{B}$ are in **Prop**, then so are $(\neg A)$ and $(\mathscr{A} \vee \mathscr{B})$. □

[†] Interestingly, our myope *can* see the brackets and the Boolean connectives.

**I.3.3 Metatheorem. Prop = Wff.**

*Proof.* $\subseteq$: We do induction on **Prop**. Every item in I.3.2(1) is in **Wff**. **Wff** satisfies I.3.2(2) (see I.1.8(b)). Done.

$\supseteq$: We do induction on **Wff**. Every item in I.1.8(a) is a propositional variable (over $\mathscr{V}$), and hence is in **Prop**.

**Prop** trivially satisfies I.1.8(b). It also satisfies I.1.8(c), for if $\mathscr{A}$ is in **Prop**, then it is in **Wff** by the $\subseteq$-direction above. Then, by I.3.1, $((\exists x)\mathscr{A})$ is a propositional variable, and hence in **Prop**.

We are done once more. □

**I.3.4 Definition (Propositional Valuations).** We can arbitrarily assign a value of 0 or 1 to every $\mathscr{A}$ in **Wff** (or **Prop**) as follows:

(1) We *fix* an assignment of 0 or 1 to *every prime formula*. We can think of this as an arbitrary but fixed function $v : \{\text{all prime formulas over } L\} \to \{0, 1\}$ in the metatheory.

(2) We define by recursion *an extension of* $v$, denoted by $\bar{v}$:

$$\bar{v}((\neg\mathscr{A})) = 1 - \bar{v}(\mathscr{A})$$
$$\bar{v}((\mathscr{A} \vee \mathscr{B})) = \bar{v}(\mathscr{A}) \cdot \bar{v}(\mathscr{B})$$

where "·" above denotes number multiplication.

We call, traditionally, the values 0 and 1 by the names "true" and "false" respectively, and write **t** and **f** respectively.

We also call a valuation $v$ a *truth (value) assignment.*

We use the jargon "$\mathscr{A}$ takes the truth value **t** (respectively, **f**) under a valuation $v$" to mean "$\bar{v}(\mathscr{A}) = 0$ (respectively, $\bar{v}(\mathscr{A}) = 1$)". □

The above inductive definition of $\bar{v}$ relies on the fact that Definition I.3.2 of **Prop** is unambiguous (I.2.10, p. 25), so that a propositional formula is *uniquely readable* (or *parsable*) (see Exercises I.5 and I.6). It employs the metatheorem on recursive definitions (I.2.13).

The reader may think that all this about unique readability is just an annoying quibble. Actually it can be a matter of life or death. The ancient Oracle of Delphi had the nasty habit of issuing ambiguous – not uniquely readable, that is – pronouncements. One famous such pronouncement, rendered in English, went like this: "You will go you will return not dying in the war".[†] Given that

[†] The original was "*Ιξεις αφιξεις ου θνηξεις εν πολεμῳ*".

ancient Greeks did not use punctuation, the above has two diametrically opposite meanings depending on whether you put a comma before or after "not".

The situation with formulas in **Prop** would have been as disastrous in the absence of brackets – which serve as punctuation – because unique readability would then not be guaranteed: For example, for three distinct prime formulas $p, q, r$ we could find a $v$ such that $\overline{v}(p \to q \to r)$ depended on whether we meant to insert brackets around "$p \to q$" or around "$q \to r$" (can you find such a $v$?).

**I.3.5 Remark (Truth Tables).** Definition I.3.4 is often given in terms of *truth functions*. For example, we could have defined (in the metatheory, of course) the function $F_\neg : \{\mathbf{t}, \mathbf{f}\} \to \{\mathbf{t}, \mathbf{f}\}$ by

$$F_\neg(x) = \begin{cases} \mathbf{t} & \text{if } x = \mathbf{f} \\ \mathbf{f} & \text{if } x = \mathbf{t} \end{cases}$$

We could then say that $\bar{v}((\neg \mathscr{A})) = F_\neg(\bar{v}(\mathscr{A}))$. One can similarly take care of all the connectives ($\vee$ and all the abbreviations) with the help of truth functions $F_\vee$, $F_\wedge$, $F_\to$, $F_\leftrightarrow$. These functions are conveniently given via so-called *truth tables* as indicated below:

| $x$ | $y$ | $F_\neg(x)$ | $F_\vee(x, y)$ | $F_\wedge(x, y)$ | $F_\to(x, y)$ | $F_\leftrightarrow(x, y)$ |
|---|---|---|---|---|---|---|
| **f** | **f** | **t** | **f** | **f** | **t** | **t** |
| **f** | **t** | **t** | **t** | **f** | **t** | **f** |
| **t** | **f** | **f** | **t** | **f** | **f** | **f** |
| **t** | **t** | **f** | **t** | **t** | **t** | **t** |

□

**I.3.6 Definition (Tautologies, Satisfiable Formulas, Unsatisfiable Formulas in Wff).** A formula $\mathscr{A} \in$ **Wff** (equivalently, in **Prop**) is a *tautology* iff for all valuations $v$, $\bar{v}(\mathscr{A}) = \mathbf{t}$.

We call the set of all tautologies, as defined here, **Taut**. The symbol $\models_{\mathbf{Taut}} \mathscr{A}$ says "$\mathscr{A}$ is in **Taut**".

A formula $\mathscr{A} \in$ **Wff** (equivalently, in **Prop**) is *satisfiable* iff for some valuation $v$, $\bar{v}(\mathscr{A}) = \mathbf{t}$. We say that $v$ *satisfies* $\mathscr{A}$.

A *set* of formulas $\Gamma$ is *satisfiable* iff for some valuation $v$, $\bar{v}(\mathscr{A}) = \mathbf{t}$ for every $\mathscr{A}$ in $\Gamma$. We say that $v$ *satisfies* $\Gamma$.

A formula $\mathscr{A} \in$ **Wff** (equivalently, in **Prop**) is *unsatisfiable* iff for all valuations $v$, $\bar{v}(\mathscr{A}) = \mathbf{f}$. A *set* of formulas $\Gamma$ is unsatisfiable iff for all valuations $v$, $\bar{v}(\mathscr{A}) = \mathbf{f}$ for some $\mathscr{A}$ in $\Gamma$. □

☡ "Satisfiable" and "unsatisfiable" are terms introduced here in the *propositional* or *Boolean* sense. These terms have a more complicated meaning when we decide to "see" the object variables and quantifiers that occur in formulas. ☡

**I.3.7 Definition (Tautologically Implies, for Formulas in Wff).** Let $\mathscr{A}$ and $\Gamma$ be respectively any formula and any set of formulas (over $L$). The symbol $\Gamma \models_{\mathbf{Taut}} \mathscr{A}$, pronounced "$\Gamma$ *tautologically implies* $\mathscr{A}$", means that every truth assignment $v$ that satisfies $\Gamma$ also satisfies $\mathscr{A}$. □

We have at once

**I.3.8 Lemma.**[†] $\Gamma \models_{\mathbf{Taut}} \mathscr{A}$ *iff* $\Gamma \cup \{\neg\mathscr{A}\}$ *is unsatisfiable (in the propositional sense).*

☡ If $\Gamma = \emptyset$, then $\Gamma \models_{\mathbf{Taut}} \mathscr{A}$ says just $\models_{\mathbf{Taut}} \mathscr{A}$, since the hypothesis "every truth assignment $v$ that satisfies $\Gamma$", in the definition above, is *vacuously* satisfied. For that reason we almost never write $\emptyset \models_{\mathbf{Taut}} \mathscr{A}$ and write instead $\models_{\mathbf{Taut}} \mathscr{A}$. ☡

☡ **I.3.9 Exercise.** For any formula $\mathscr{A}$ and any two valuations $v$ and $v'$, $\bar{v}(\mathscr{A}) = \bar{v}'(\mathscr{A})$ if $v$ and $v'$ agree on all the propositional variables that occur in $\mathscr{A}$.

In the same manner, $\Gamma \models_{\mathbf{Taut}} \mathscr{A}$ is oblivious to $v$-variations that do not affect the variables that occur in $\Gamma$ and $\mathscr{A}$ (see Exercise I.7). □ ☡

Before presenting the axioms, we need to introduce the concept of *substitution*.

**I.3.10 Tentative Definition (Substitution of a Term for a Variable).** Let $\mathscr{A}$ be a formula, $x$ an (object) variable, and $t$ a term.

$\mathscr{A}[x \leftarrow t]$ denotes the result of "replacing" all free occurrences of $x$ in $\mathscr{A}$ by the term $t$, provided no variable of $t$ was "captured" (by a quantifier) during

[†] The word "lemma" has Greek origin, "λήμμα", plural "lemmata" – many people say "lemmas" – from "Λήμματα". It derives from the verb "λαμβάνω" (to take) and thus means "taken thing". In mathematical reasoning a lemma is a provable auxiliary statement that is *taken* and used as a stepping stone in lengthy mathematical arguments – invoked therein by name, as in "... by Lemma such and such ..." – much as subroutines (or procedures) are taken and used as auxiliary stepping stones to elucidate lengthy computer programs. Thus our purpose in having lemmata is to shorten proofs by breaking them up into modules.

substitution. If the proviso *is* valid, then we say that "$t$ is *substitutable for* $x$ (in $\mathscr{A}$)", or that "$t$ is *free for* $x$ (in $\mathscr{A}$)".

If the proviso is not valid, then the substitution is undefined. □

**I.3.11 Remark.** There are a number of issues about Definition I.3.10 that need discussion or clarification.

Any reasonable person will be satisfied with the above definition "as is". However, there are some obscure points (deliberately quoted, above).

(1) What is this about "capture"? Well, suppose that $\mathscr{A} \equiv (\exists x)\neg x = y$. Let $t \equiv x$.[†] Then, if we ignore the provison in I.3.10, $\mathscr{A}[y \leftarrow t] \equiv (\exists x)\neg x = x$, which says something altogether different than the original. Intuitively, this is unexpected (and undesirable): $\mathscr{A}$ codes a statement about the free variable $y$, i.e., a statement about all objects which could be values (or meanings) of $y$. One would have expected that, in particular, $\mathscr{A}[y \leftarrow x]$ – *if the substitution were allowed* – would make this very same statement about the values of $x$. It does not.[‡] What happened is that $x$ was *captured by the quantifier* upon substitution, thus distorting $\mathscr{A}$'s original meaning.

(2) Are we sure that the term "replace" is mathematically precise?

(3) Is $\mathscr{A}[x \leftarrow t]$ always a formula, if $\mathscr{A}$ is?

A revisitation of I.3.10 via an inductive definition (by induction on terms and formulas) settles (1)–(3) at once (in particular, the intuitive terms "replace" and "capture" do not appear in the inductive definition). Here it goes:

First off, let us define $s[x \leftarrow t]$, where $s$ is also a term, by cases:

$$s[x \leftarrow t] \equiv \begin{cases} t & \text{if } s \equiv x \\ a & \text{if } s \equiv a, \text{ a constant} \\ & \qquad\text{(symbol)} \\ y & \text{if } s \equiv y, \text{ a variable } \not\equiv x \\ f r_1[x \leftarrow t] r_2[x \leftarrow t] \ldots r_n[x \leftarrow t] & \text{if } s \equiv f r_1 \ldots r_n \end{cases}$$

**Pause.** Is $s[x \leftarrow t]$ always a term? That this is so follows directly by induction on terms, using the definition by cases above and the I.H. that each of $r_i[x \leftarrow t]$, $i = 1, \ldots, n$, is a term.

[†] Recall that in I.1.4 (p. 13) we defined the symbol "$\equiv$" to be equality on strings. No further reminders will be issued.

[‡] And that is why the substitution is not allowed. The original formula says that for any object $y$ there is an object that is different from it. On the other hand, $\mathscr{A}[y \leftarrow x]$ says that there is an object that is different from itself.

We turn now to formulas. The symbols $P, r, s$ (with or without subscripts) below denote a predicate of arity $n$, a term and a term (respectively).

$$\mathscr{A}[x \leftarrow t] \equiv \begin{cases} s[x \leftarrow t] = r[x \leftarrow t] & \text{if } \mathscr{A} \equiv s = r \\ Pr_1[x \leftarrow t]r_2[x \leftarrow t]\ldots r_n[x \leftarrow t] & \text{if } \mathscr{A} \equiv Pr_1 \ldots r_n \\ (\mathscr{B}[x \leftarrow t] \vee \mathscr{C}[x \leftarrow t]) & \text{if } \mathscr{A} \equiv (\mathscr{B} \vee \mathscr{C}) \\ \big(\neg(\mathscr{B}[x \leftarrow t])\big) & \text{if } \mathscr{A} \equiv (\neg\mathscr{B}) \\ \mathscr{A} & \text{if } \mathscr{A} \equiv ((\exists y)\mathscr{B}) \text{ and } \\ & \quad y \equiv x \\ \big((\exists y)(\mathscr{B}[x \leftarrow t])\big) & \text{if } \mathscr{A} \equiv ((\exists y)\mathscr{B}) \text{ and } \\ & \quad y \not\equiv x \text{ and } y \text{ does} \\ & \qquad \text{not occur in } t \end{cases}$$

In all cases above, the left hand side is defined iff the right hand side is.

**Pause.** We have eliminated "replaces" and "captured". Is though $\mathscr{A}[x \leftarrow t]$ a formula (whenever it is defined)? (See Exercise I.8.) □

**I.3.12 Definition (Simultaneous Substitution).** The symbols $\mathscr{A}[y_1, \ldots, y_r \leftarrow t_1, \ldots, t_r]$ or, equivalently, $\mathscr{A}[\vec{y}_r \leftarrow \vec{t}_r]$ – where $\vec{y}_r$ is an abbreviation of $y_1, \ldots, y_r$ – denote *simultaneous substitution* of the terms $t_1, \ldots, t_r$ into the variables $y_1, \ldots, y_r$ in the following sense: Let $\vec{z}_r$ be variables that do not occur at all (either as free or bound) in either $\mathscr{A}$ or $\vec{t}_r$. Then $\mathscr{A}[\vec{y}_r \leftarrow \vec{t}_r]$ is short for

$$\mathscr{A}[y_1 \leftarrow z_1]\ldots[y_r \leftarrow z_r][z_1 \leftarrow t_1]\ldots[z_r \leftarrow t_r] \tag{1}$$

□

Exercise I.9 shows that we obtain the same string in (1) above, regardless of our choice of new variables $\vec{z}_r$.

***More conventions***: The symbol $[x \leftarrow t]$ lies in the metalanguage. This metasymbol has the highest priority, so that, e.g., $\mathscr{A} \vee \mathscr{B}[x \leftarrow t]$ means $\mathscr{A} \vee (\mathscr{B}[x \leftarrow t])$, $(\exists x)\mathscr{B}[x \leftarrow t]$ means $(\exists x)(\mathscr{B}[x \leftarrow t])$, etc.

We often write $\mathscr{A}[y_1, \ldots, y_r]$, rather than the terse $\mathscr{A}$, in order to convey our interest in the *free* variables $y_1, \ldots, y_r$ that *may or may not actually appear free in* $\mathscr{A}$. Other variables, not mentioned in the notation, may also be free in $\mathscr{A}$ (see also I.1.11).

*In this context*, if $t_1, \ldots, t_r$ are terms, the symbol $\mathscr{A}[t_1, \ldots, t_r]$ abbreviates $\mathscr{A}[\vec{y}_r \leftarrow \vec{t}_r]$.

We are ready to introduce the (logical) axioms and rules of inference.

**Schemata.**[†] Some of the axioms below will actually be *schemata*. A *formula schema*, or *formula form*, is a string $\mathscr{S}$ of the metalanguage that contains *syntactic variables* (or metavariables), such as $\mathscr{A}$, $P$, $f$, $a$, $t$, $x$.

Whenever we replace all these syntactic variables that occur in $\mathscr{S}$ by specific formulas, predicates, functions, constants, terms, or variables respectively, we obtain a specific well-formed formula, a so-called *instance of the schema*. For example, an instance of $(\exists x)x = a$ is $(\exists v_{12})v_{12} = 0$ (in the language of Peano arithmetic). An instance of $\mathscr{A} \to \mathscr{A}$ is $v_{101} = v_{114} \to v_{101} = v_{114}$.

**I.3.13 Definition (Axioms and Axiom Schemata).** The *logical axioms* are all the formulas in the group **Ax1** and all the possible instances of the schemata in the remaining groups:

**Ax1.** All formulas in **Taut**.
**Ax2.** (*Substitution axiom. Schema*)

$$\mathscr{A}[x \leftarrow t] \to (\exists x)\mathscr{A} \qquad \text{for any term } t.$$

By I.3.10–I.3.11, the notation already imposes a condition on $t$, that it is substitutable for $x$.

N.B. We often see the above written as

$$\mathscr{A}[t] \to (\exists x)\mathscr{A}[x]$$

or even

$$\mathscr{A}[t] \to (\exists x)\mathscr{A}$$

**Ax3.** (*Schema*) For *each* object variable $x$, the formula $x = x$.
**Ax4.** (*Leibniz's characterization of equality – first order version. Schema*) For any formula $\mathscr{A}$, object variable $x$, and any terms $t$ and $s$, the formula

$$t = s \to (\mathscr{A}[x \leftarrow t] \leftrightarrow \mathscr{A}[x \leftarrow s])$$

N.B. The above is written usually as

$$t = s \to (\mathscr{A}[t] \leftrightarrow \mathscr{A}[s])$$

as long as we remember that the notation already requires that $t$ and $s$ be free for $x$. We will denote the above set of logical axioms $\Lambda$. □

[†] Plural of *schema*. This is of Greek origin, σχήμα, meaning – e.g., in geometry – figure or configuration or even formation.

The logical axioms for equality are not the strongest possible, but they are adequate for the job. What Leibniz really proposed was the schema $t = s \leftrightarrow (\forall P)(P[t] \leftrightarrow P[s])$, which says, intuitively, that "two objects $t$ and $s$ are equal iff, for every property $P$, both have $P$ or neither has $P$".

Unfortunately, our system of notation (first-order language) does not allow quantification over predicate symbols (which can have as "values" arbitrary "properties"). But is not **Ax4** read "for all formulas $\mathscr{A}$" anyway? Yes, but with one qualification: "For all formulas $\mathscr{A}$ *that we can write down in our system of notation*", and, alas, we cannot write *all* possible formulas of *real mathematics* down, because they are too many.[†]

While the symbol "=" is suggestive of equality, it is *not* its shape that qualifies it. It is the two axioms, **Ax3** and **Ax4**, that make the symbol *behave* as we expect equality to behave, and any other symbol of any other shape (e.g., Enderton (1972) uses "$\approx$") satisfying these two axioms *qualifies* as *formal equality* that is intended to codify the metamathematical standard "=".

**I.3.14 Remark.** In **Ax2** and **Ax4** we imposed the condition that $t$ (and $s$) must be substitutable in $x$. Here is why:

Take $\mathscr{A}$ to stand for $(\forall y)x = y$ and $\mathscr{B}$ to stand for $(\exists y)\neg x = y$. Then, *temporarily suspending the restriction on substitutability*, $\mathscr{A}[x \leftarrow y] \rightarrow (\exists x)\mathscr{A}$ is

$$(\forall y)y = y \rightarrow (\exists x)(\forall y)x = y$$

and $x = y \rightarrow \big(\mathscr{B} \leftrightarrow \mathscr{B}[x \leftarrow y]\big)$ is

$$x = y \rightarrow \big((\exists y)\neg x = y \leftrightarrow (\exists y)\neg y = y\big)$$

neither of which, obviously, is "valid".[‡]

There is a remedy in the metamathematics: That is, move the quantified variable(s) out of harm's way, by renaming them so that no quantified variable in $\mathscr{A}$ has the same name as any (free, of course) variable in $t$ (or $s$).

This renaming is formally correct (i.e., it does not change the meaning of the formula) as we will see in the *variant* (meta)theorem I.4.13. Of course, it is always possible to effect this renaming, since we have countably many variables, and only finitely many appear free in $t$ (and $s$) and $\mathscr{A}$.

[†] *Uncountably* many, in a precise technical sense that we will introduce in Chapter VII. This is due to Cantor's theorem, which implies that there are uncountably many subsets of $\mathbb{N}$. Each such subset $A$, gives rise to the formula, $x \in A$, *in the metalanguage*.

On the other hand, our formal system of notation, using just $\in$ and $U$ as start-up (nonlogical) symbols, is not rich enough to write down but a *countably infinite* set of formulas (at some point later, Example VII.5.17, this will be clear). Thus, our notation will fail to denote uncountably many "real formulas" $x \in A$.

[‡] Speaking intuitively is enough for now. Validity will be defined carefully pretty soon.

This trivial remedy allows us to render the conditions in **Ax2** and **Ax4** harmless. Essentially, a $t$ (or $s$) is always substitutable *after renaming*. □

**I.3.15 Definition (Rules of Inference).** The following two are the only *primitive*[†] *rules of inference*. These rules are *relations* with inputs from the set **Wff** and outputs also in **Wff**. They are written down, traditionally, as "fractions" through the employment of *syntactic (or meta-) variables*. We call the "numerator" the *premise(s)* and the "denominator" the *conclusion*.

We say that a rule of inference is *applied* to any *instance* of the formula schema(ta) in the numerator, and that it *yields* (or *results in*) the *corresponding instance*[‡] of the formula schema in the denominator.

**Inf1.** *Modus ponens*, or MP, is the rule

$$\frac{\mathscr{A}, \mathscr{A} \to \mathscr{B}}{\mathscr{B}}$$

**Inf2.** $\exists$-*introduction* – pronounced *E-introduction* – is the rule

$$\frac{\mathscr{A} \to \mathscr{B}}{(\exists x)\mathscr{A} \to \mathscr{B}}$$

that is applicable if a *side condition* is met: That $x$ is *not* free in $\mathscr{B}$.

N.B. Recall the conventions on eliminating brackets. □

It is immediately clear that the definition above meets our requirement that the rules of inference be "algorithmic", in the sense that *whether* they are applicable can be decided and their application can be carried out in a finite number of steps by just looking at the *form* of (potential input) formulas (not at their meaning).

We next define $\Gamma$-theorems, that is, formulas we can *prove from* the *set* of formulas $\Gamma$ (this $\Gamma$ may be empty).

**I.3.16 Definition ($\Gamma$-Theorems).** The set of $\Gamma$-*theorems*, $\mathbf{Thm}_\Gamma$, is the least inclusive subset of **Wff** that satisfies

**Th1.** $\Lambda \subseteq \mathbf{Thm}_\Gamma$ (see I.3.13).
**Th2.** $\Gamma \subseteq \mathbf{Thm}_\Gamma$. We call every member of $\Gamma$ a *nonlogical axiom*.
**Th3.** $\mathbf{Thm}_\Gamma$ is *closed under* each rule **Inf1–Inf2**.

[†] That is, given initially. Other rules can be proved to hold, and we call them *derived rules*.

[‡] The corresponding instance is the one obtained from the schema in the denominator by replacing each of its metavariables by the *same* specific formula, or term, used to instantiate all the occurrences of the same metavariable in the numerator.

The metalinguistic statement $\mathscr{A} \in \mathbf{Thm}_\Gamma$ is traditionally written as $\Gamma \vdash \mathscr{A}$, and we say that $\mathscr{A}$ *is proved from* $\Gamma$ or that it is a $\Gamma$*-theorem.*

We also say that $\mathscr{A}$ is *deduced* from $\Gamma$, or that $\Gamma$ *deduces* $\mathscr{A}$.

If $\Gamma = \emptyset$, then rather than $\emptyset \vdash \mathscr{A}$ we write $\vdash \mathscr{A}$. We often say in this case that $\mathscr{A}$ is *absolutely provable* (or *provable with no nonlogical axioms*).

We often write $\mathscr{A}, \mathscr{B}, \ldots, \mathscr{D} \vdash \mathscr{E}$ for $\{\mathscr{A}, \mathscr{B}, \ldots, \mathscr{D}\} \vdash \mathscr{E}$. □

**I.3.17 Definition ($\Gamma$-Proofs).** We just saw that $\mathbf{Thm}_\Gamma = \mathrm{Cl}(\mathscr{I}, \mathscr{R})$, where $\mathscr{I} = \Lambda \cup \Gamma$ and $\mathscr{R}$ contains just the two rules of inference. A $(\mathscr{I}, \mathscr{R})$-derivation is also called a $\Gamma$-*proof* (or just proof, if $\Gamma$ is understood). □

**I.3.18 Remark.** (1) It is clear that if each of $\mathscr{A}_1, \ldots, \mathscr{A}_n$ has a $\Gamma$-proof and $\mathscr{B}$ has an $\{\mathscr{A}_1, \ldots, \mathscr{A}_n\}$-proof, then $\mathscr{B}$ has a $\Gamma$-proof. Indeed, simply concatenate each of the given $\Gamma$-proofs (in any sequence). Append to the right of that sequence the given $\{\mathscr{A}_1, \ldots, \mathscr{A}_n\}$-proof (that ends with $\mathscr{B}$). Then the entire sequence is a $\Gamma$-proof, and ends with $\mathscr{B}$.

We refer to this phenomenon as the *transitivity of* $\vdash$.

*Very important.* Transitivity of $\vdash$ allows one to invoke previously proved (by oneself or others) *theorems* in the course of a proof. Thus, *practically*, a $\Gamma$-proof is a sequence of formulas in which each formula is an axiom, is a known $\Gamma$-theorem, or is obtained by applying a rule of inference to previous formulas of the sequence.

(2) If $\Gamma \subseteq \Delta$ and $\Gamma \vdash \mathscr{A}$, then also $\Delta \vdash \mathscr{A}$, as follows from I.3.16 or I.3.17. In particular, $\vdash \mathscr{A}$ implies $\Gamma \vdash \mathscr{A}$ for any $\Gamma$.

(3) It is immediate from the definitions that for any formulas $\mathscr{A}$ and $\mathscr{B}$,

$$\mathscr{A}, \mathscr{A} \to \mathscr{B} \vdash \mathscr{B} \tag{$i$}$$

and, if, moreover, $x$ is not free in $\mathscr{B}$,

$$\mathscr{A} \to \mathscr{B} \vdash (\exists x)\mathscr{A} \to \mathscr{B} \tag{$ii$}$$

Some texts (e.g., Schütte (1977)) give the rules in the format of ($i$)–($ii$) above. □

The axioms and rules provide us with a *calculus*, that is, a means to "calculate" (used synonymously with *construct*) proofs and theorems. In the interest of making the calculus more user-friendly – and thus more easily applicable to mathematical theories of interest, such as set theory – we are going to develop in the next section a number of "derived principles". These principles are largely of the form $\mathscr{A}_1, \ldots, \mathscr{A}_n \vdash \mathscr{B}$. We call such a (provable in the metatheory) principle a *derived rule of inference*, since, by transitivity of $\vdash$, it can be used as a proof step in a $\Gamma$-proof. By contrast, the rules **Inf1–Inf2** are "primitive" (or "basic" or "primary"); they are given outright.

We can now fix our understanding of the concept of a formal or mathematical *theory*.

A *(first order) formal (mathematical) theory*, or just *theory over a language* $L$, or just *theory*, is a tuple (of "ingredients") $\mathfrak{T} = (L, \Lambda, \mathbf{I}, \mathscr{T})$, where $L$ is a first order language, $\Lambda$ is a set of *logical axioms*, $\mathbf{I}$ is a set of rules of inference, and $\mathscr{T}$ a *non-empty* subset of **Wff** that is required to contain $\Lambda$ (i.e., $\Lambda \subseteq \mathscr{T}$) and be closed under the rules $\mathbf{I}$.

Equivalently, one may simply require that $\mathscr{T}$ be *closed under* $\vdash$, that is,

$$\text{for any } \Gamma \subseteq \mathscr{T} \text{ and any formula } \mathscr{A}, \qquad \text{if } \Gamma \vdash \mathscr{A}, \text{ then } \mathscr{A} \in \mathscr{T}.$$

This is, furthermore, equivalent to requiring that

$$\mathscr{A} \in \mathscr{T} \quad \text{iff} \quad \mathscr{T} \vdash \mathscr{A} \tag{1}$$

Indeed, the if direction follows from closure under $\vdash$, while the only-if direction is a consequence of Definition I.3.16.

$\mathscr{T}$ is the set of the formulas *of the theory*,[†] and we often say "a theory $\mathscr{T}$", taking everything else for granted.

If $\mathscr{T} = \mathbf{Wff}$, then the theory $\mathfrak{T}$ is called *inconsistent* or *contradictory*. Otherwise it is called *consistent*.

*Throughout our exposition we fix* $\Lambda$ *and* $\mathbf{I}$ *as in Definitions* I.3.13 *and* I.3.15. By (1), $\mathscr{T} = \mathbf{Thm}_{\mathscr{T}}$. This observation suggests that we call theories – such as the ones we have just defined – *axiomatic theories*, in that a set $\Gamma$ always exists such that $\mathscr{T} = \mathbf{Thm}_\Gamma$ (if at a loss, we can just take $\Gamma = \mathscr{T}$).

We are mostly interested in theories $\mathfrak{T}$ for which there is a "small" set $\Gamma$ ("small" by comparison with $\mathscr{T}$) such that $\mathscr{T} = \mathbf{Thm}_\Gamma$. We say that $\mathfrak{T}$ is *axiomatized* by $\Gamma$. Naturally, we call $\mathscr{T}$ the set of *theorems*, and $\Gamma$ the set of *nonlogical* axioms, of $\mathfrak{T}$.

If, moreover, $\Gamma$ is "recognizable" (i.e., we can tell "algorithmically" whether or not a formula $\mathscr{A}$ is in $\Gamma$), then we say that $\mathfrak{T}$ is *recursively axiomatized*.

Examples of recursively axiomatized theories are ZFC set theory and Peano arithmetic. On the other hand, if we take $\mathscr{T}$ to be all the sentences of arithmetic

[†] As opposed to "of the language", which is all of **Wff**.

that are true when interpreted "in the standard way"[†] over $\mathbb{N}$ – the so-called *complete arithmetic* – then there is *no* recognizable $\Gamma$ such that $\mathscr{T} = \mathbf{Thm}_\Gamma$. We say that complete arithmetic is not *recursively axiomatizable*.[‡]

**Pause.** Why does complete arithmetic form a theory? Because work of the next section – in particular, the soundness theorem – entails that it is closed under $\vdash$.

We tend to further abuse language and call axiomatic theories by the name of their (set of) nonlogical axioms $\Gamma$. Thus if $\mathfrak{T} = (L, \Lambda, \mathbf{I}, \mathscr{T})$ is a first order theory and $\mathscr{T} = \mathbf{Thm}_\Gamma$, then we may say interchangeably "theory $\mathfrak{T}$", "theory $\mathscr{T}$", or "theory $\Gamma$".

If $\Gamma = \emptyset$, then we have a *pure* or *absolute* theory (i.e., we are "just doing logic, not math"). If $\Gamma \neq \emptyset$ then we have an *applied* theory.

***Argot.*** *A* final *note on language versus metalanguage, and theory versus metatheory*. When are we speaking the metalanguage, and when are we speaking the formal language?

The answers are, respectively, "almost always" and "almost never". As has been remarked before, *in principle*, we are speaking the formal language exactly when we are pronouncing or writing down a string from **Term** or **Wff**. Otherwise we are (speaking or writing) in the metalanguage. It appears that we (and everybody else who has written a book in logic or set theory) are speaking and writing within the metalanguage with a frequency approaching 100%.

The formalist is clever enough to simplify notation at all times. We will seldom be caught writing down a member of **Wff** in this book, and, on the rare occasions we may do so, it will only be to serve as an illustration of why one should avoid writing down such formulas: because they are too long and hard to read and understand.

We will be speaking the formal language with a heavy "accent" and using many idioms borrowed from "real" (meta-) mathematics, and English. We will call our dialect *argot*, following Manin (1977).

A related, and practically more important,[§] question is "When are we arguing in the *theory*, and when are we arguing in the *metatheory*?". That is, the question is not about how we speak, but about what we are saying when we speak.

[†] That is, the symbol "0" of the language is interpreted as $0 \in \mathbb{N}$, "$Sx$" as $x + 1$, "$(\exists x)$" as "there is an $x \in \mathbb{N}$", etc.

[‡] The trivial "solution", that is, taking $\Gamma = \mathscr{T}$, will not do, for $\mathscr{T}$ is not recognizable.

[§] Important, because arguing in the theory restricts us to use *only* its axioms (and earlier proved theorems; cf. I.3.18) and its rules of inference – nothing extraneous to these syntactic tools is allowed.

The answer to this is also easy: Once we have fixed a theory $\mathfrak{T}$ and the nonlogical axioms $\Gamma$, we are working in the theory iff we are writing down a ($\Gamma$-) proof of some specific formula $\mathscr{A}$. It does not matter if $\mathscr{A}$ (and much of the what we write down during the proof) is in *argot*.

Two examples:

(1) One is working *in* formal number theory (or formal arithmetic) if one states and proves (say, from the Peano axioms) that "every natural number $n > 1$ has a prime factor". Note how this theorem is stated in *argot*. Below we give its translation into the formal language of arithmetic:[†]

$$\begin{aligned}(\forall n)\big(S0 < n \to (\exists x)(\exists y)\big(n = x \times y \wedge \\ S0 < x \wedge (\forall m)(\forall r)(x = m \times r \to m = S0 \vee m = x)\big)\big)\end{aligned} \tag{1}$$

(2) One is working in formal logic if one is writing a proof of $(\exists v_{13})v_{13} = v_{13}$.

Suppose though that our activity consists of effecting definitions, introducing axioms, or analyzing the behaviour or capability of $\mathfrak{T}$, e.g., proving some derived rule $\mathscr{A}_1, \ldots, \mathscr{A}_n \vdash \mathscr{B}$ – that is, a *theorem schema* – or investigating consistency,[‡] or *relative consistency*.[§] Then we are operating in the *metatheory*, that is, in "real" mathematics. ☡

☡☡ One of the most important problems posed in the metatheory is

"Given a theory $\mathfrak{T}$ and a formula $\mathscr{A}$. Is $\mathscr{A}$ a theorem of $\mathfrak{T}$?"

This is Hilbert's *Entscheidungsproblem*, or *decision problem*. Hilbert believed that every recursively axiomatized theory ought to admit a "general" solution, by more or less "mechanical means", to its decision problem. The techniques of Gödel and the insight of Church showed that this problem is, in general, algorithmically unsolvable.

As we have already stated, metamathematics exists outside and independently of our effort to build this or that formal system. All its methods are – in principle – available to us for use in the analysis of the behaviour of a formal system.

[†] Well, almost. In the interest of brevity, all the variable names used in the displayed formula (1) are metasymbols.

[‡] That is, whether or not $\mathscr{T} = \mathbf{Wff}$.

[§] That is, "if $\Gamma$ is consistent," – where we are naming the theory by its nonlogical axioms – "does it stay so after we have added some formula $\mathscr{A}$ as a nonlogical axiom?".

**Pause.** But how much of real mathematics are we allowed to use, *reliably*, to study or speak about the "simulator" that the formal system is?[†]

For example, have we not overstepped our license by using induction (and, implicitly, the entire *infinite* set $\mathbb{N}$), specifically the recursive definitions of terms, well-formed formulas, theorems, etc.?

The quibble here is largely "political". Some people argue (a major proponent of this was Hilbert) as follows: Formal mathematics was meant to crank out "true" statements of mathematics, but no "false" ones, and this freedom of contradiction ought to be verifiable.

Now, as we are verifying so in the metatheory (i.e., outside the formal system), shouldn't the metatheory itself be above suspicion (of contradiction, that is)? Naturally.

Hilbert's suggestion towards achieving this "above suspicion" status was, essentially, to utilize in the metatheory only a small fragment of "reality" that is so simple and close to intuition that it does not need itself any "certificate" (via formalization) for its freedom from contradiction.

In other words, restrict the metamathematics![‡]

Such a fragment of the metatheory, he said, should have nothing to do with the "infinite", in particular with the entire set $\mathbb{N}$ and all that it entails (e.g., inductive definitions and proofs).[§]

If it were not for Gödel's incompleteness results, this position – that metamathematical techniques must be finitary – might have prevailed. However, Gödel proved it to be futile, and most mathematicians have learnt to feel comfortable with infinitary metamathematical techniques, or at least with $\mathbb{N}$ and induction.[¶] Of course, it would be imprudent to use as metamathematical tools mathematics of suspect consistency (e.g., the *full* naïve theory of sets).

[†] The methods or scope of the metamathematics that a logician uses – in the investigation of some formal system – are often *restricted* for technical or philosophical reasons.

[‡] Otherwise we would need to formalize the metamathematics – in order to "certify" it – and next the metametamathematics, and so on. For if "metaM" is to authoritatively check "M" for consistency, then it too must be consistent; so let us formalize "metaM" and let "metametaM" check it; ... – a never ending story.

[§] See Hilbert and Bernays (1968, pp. 21–29) for an elaborate scheme that constructs "concrete number objects" – *Ziffern* or "numerals" – "|","||","|||", etc., that stand for "1","2","3", etc., complete with a "concrete mathematical induction" proof technique on these objects, and even the beginnings of their "recursion theory". Of course, at any point, only finite sets of such objects were considered.

[¶] Some proponents of infinitary techniques in metamathematics have used very strong words in describing the failure of Hilbert's program. Rasiowa and Sikorski (1963) write in their introduction: "However Gödel's results exposed the fiasco of Hilbert's finitistic methods as far as consistency is concerned."

It is worth pointing out that one could fit (with some effort) our inductive definitions within Hilbert's style. But we will not do so.

First, one would have to abandon the elegant (and now widely used) approach with *closures*, and use instead the concept of *derivations* of Section I.2.

Then one would somehow have to effect and study derivations without the benefit of the *entire* set $\mathbb{N}$. Bourbaki (1966b, p. 15) does so with his *constructions formatives*. Hermes (1973) is another author who does so, with his "term-" and "formula-calculi" (such calculi being, essentially, *finite* descriptions of derivations).

Bourbaki (but not Hermes) avoids induction over all of $\mathbb{N}$. In his metamathematical discussions of terms and formulas[†] that are derived by a derivation $d_1, \ldots, d_n$, he restricts his induction arguments to the segment $\{0, 1, \ldots, n\}$, that is, he takes an I.H. on $k < n$ and proceeds to $k + 1$.

## I.4. Basic Metatheorems

We are dealing with an arbitrary theory $\mathfrak{T} = (L, \Lambda, \mathbf{I}, \mathscr{T})$, such that $\Lambda$ is the set of logical axioms I.3.13 and $\mathbf{I}$ are the inference rules I.3.15. We also let $\Gamma$ be an appropriate set of nonlogical axioms, i.e., $\mathscr{T} = \mathbf{Thm}_\Gamma$.

**I.4.1 Metatheorem (Post's "Extended" Tautology Theorem).** *If* $\mathscr{A}_1, \ldots, \mathscr{A}_n \models_{\mathbf{Taut}} \mathscr{B}$ *then* $\mathscr{A}_1, \ldots, \mathscr{A}_n \vdash \mathscr{B}$.

*Proof.* The assumption yields that

$$\models_{\mathbf{Taut}} \mathscr{A}_1 \to \cdots \to \mathscr{A}_n \to \mathscr{B} \tag{1}$$

Thus – since the formula in (1) is in $\Lambda$, and using Definition I.3.16,

$$\mathscr{A}_1, \ldots, \mathscr{A}_n \vdash \mathscr{A}_1 \to \cdots \to \mathscr{A}_n \to \mathscr{B} \tag{2}$$

Applying modus ponens to (2), $n$ times, we deduce $\mathscr{B}$. □

I.4.1 is an omnipresent *derived rule*.

**I.4.2 Definition.** $\mathscr{A}$ and $\mathscr{B}$ are *provably equivalent in* $\mathfrak{T}$ means that $\Gamma \vdash \mathscr{A} \leftrightarrow \mathscr{B}$. □

**I.4.3 Metatheorem.** *Any two theorems* $\mathscr{A}$ *and* $\mathscr{B}$ *of* $\mathfrak{T}$ *are provably equivalent in* $\mathfrak{T}$.

[†] For example, in *loc. cit.*, p. 18, where he proves that, in our notation, $\mathscr{A}[x \leftarrow y]$ and $t[x \leftarrow y]$ are a formula and term respectively.

*Proof.* By I.4.1, $\Gamma \vdash \mathscr{A}$ yields $\Gamma \vdash \mathscr{B} \rightarrow \mathscr{A}$. Similarly, $\Gamma \vdash \mathscr{A} \rightarrow \mathscr{B}$ follows from $\Gamma \vdash \mathscr{B}$. One more application of I.4.1 yields $\Gamma \vdash \mathscr{A} \leftrightarrow \mathscr{B}$. □

$\vdash \neg x = x \leftrightarrow \neg y = y$ (why?), but neither $\neg x = x$ nor $\neg y = y$ is a $\emptyset$-theorem.

**I.4.4 Remark (Hilbert Style Proofs).** In practice we write proofs "vertically", that is, as numbered vertical sequences (or lists) of formulas. The numbering helps the annotational comments that we insert to the right of each formula that we list, as the following proof demonstrates.

A metatheorem admits a *meta*proof, strictly speaking. The following is a derived rule (or theorem schema) and thus belongs to the metatheory (and so does its proof).

Another point of view is possible, however: The syntactic symbols $x$, $\mathscr{A}$, and $\mathscr{B}$ below stand for a *specific* variable and *specific* formulas that we just forgot to write down explicitly. Then one can think of the proof as a (formal) Hilbert style proof. □

**I.4.5 Metatheorem (∀-Introduction – Pronounced *A-Introduction*).** *If $x$ does not occur free in $\mathscr{A}$, then $\mathscr{A} \rightarrow \mathscr{B} \vdash \mathscr{A} \rightarrow (\forall x)\mathscr{B}$.*

*Proof.*

| | | |
|---|---|---:|
| (1) | $\mathscr{A} \rightarrow \mathscr{B}$ | given |
| (2) | $\neg\mathscr{B} \rightarrow \neg\mathscr{A}$ | (1) and I.4.1 |
| (3) | $(\exists x)\neg\mathscr{B} \rightarrow \neg\mathscr{A}$ | (2) and ∃-introduction |
| (4) | $\mathscr{A} \rightarrow \neg(\exists x)\neg\mathscr{B}$ | (3) and I.4.1 |
| (5) | $\mathscr{A} \rightarrow (\forall x)\mathscr{B}$ | (4), introducing the ∀-abbreviation |

□

**I.4.6 Metatheorem (Specialization).** *For any formula $\mathscr{A}$ and term $t$,* $\vdash (\forall x)\mathscr{A} \rightarrow A[t]$.

At this point, the reader may want to review our abbreviation conventions; in particular, see **Ax2** (I.3.13).

*Proof.*

| | | |
|---|---|---:|
| (1) | $\neg\mathscr{A}[t] \rightarrow (\exists x)\neg\mathscr{A}$ | in $\Lambda$ |
| (2) | $\neg(\exists x)\neg\mathscr{A} \rightarrow \mathscr{A}[t]$ | (1) and I.4.1 |
| (3) | $(\forall x)\mathscr{A} \rightarrow A[t]$ | (2), introducing the ∀-abbreviation |

□

**I.4.7 Corollary.** *For any formula* $\mathscr{A}$, $\vdash (\forall x)\mathscr{A} \to A$.

*Proof.* $\mathscr{A}[x \leftarrow x] \equiv \mathscr{A}$. □

**Pause.** Why is $\mathscr{A}[x \leftarrow x]$ the same string as $\mathscr{A}$?

**I.4.8 Metatheorem (Generalization).** *For any* $\Gamma$ *and any* $\mathscr{A}$, *if* $\Gamma \vdash \mathscr{A}$, *then* $\Gamma \vdash (\forall x)A$.

*Proof.* Choose $y \not\equiv x$. Then we continue any given proof of $\mathscr{A}$ (from $\Gamma$) as follows:

| | | |
|---|---|---|
| (1) | $\mathscr{A}$ | proved from $\Gamma$ |
| (2) | $y = y \to \mathscr{A}$ | (1) and I.4.1 |
| (3) | $y = y \to (\forall x)\mathscr{A}$ | (2) and $\forall$-introduction |
| (4) | $y = y$ | in $\Lambda$ |
| (5) | $(\forall x)\mathscr{A}$ | (3), (4) and MP |

□

**I.4.9 Corollary.** *For any* $\Gamma$ *and any* $\mathscr{A}$, $\Gamma \vdash \mathscr{A}$ *iff* $\Gamma \vdash (\forall x)\mathscr{A}$.

*Proof.* By I.4.7, I.4.8, and modus ponens. □

**I.4.10 Corollary.** *For any* $\mathscr{A}$, $\mathscr{A} \vdash (\forall x)\mathscr{A}$ *and* $(\forall x)\mathscr{A} \vdash \mathscr{A}$.

The above corollary motivates the following definition. It also justifies the common mathematical practice of the "implied universal quantifier". That is, we often just state "$\ldots x \ldots$" when we mean "$(\forall x) \ldots x \ldots$".

**I.4.11 Definition (Universal Closure).** Let $y_1, \ldots, y_n$ be the list of all free variables of $\mathscr{A}$. The *universal closure* of $\mathscr{A}$ is the formula $(\forall y_1)(\forall y_2) \cdots (\forall y_n)\mathscr{A}$ – often written more simply as $(\forall y_1 y_2 \ldots y_n)\mathscr{A}$ or even $(\forall \vec{y}_n)\mathscr{A}$. □

By I.4.10, a formula deduces and is deduced by its universal closure.

**Pause.** We said *the* universal closure. Hopefully, the remark immediately above is robust to permutation of $(\forall y_1)(\forall y_2) \cdots (\forall y_n)$. Is it? (Exercise 1.10.)

**I.4.12 Corollary (Substitution of Terms).** $\mathscr{A}[x_1, \ldots, x_n] \vdash \mathscr{A}[t_1, \ldots, t_n]$ *for any terms* $t_1, \ldots, t_n$.

The reader may wish to review I.3.12 and the remark following it.

*Proof.* We illustrate the proof for $n = 2$. What makes it interesting is the requirement to have "simultaneous substitution". To that end we first substitute into $x_1$ and $x_2$ *new* variables $z$, $w$ – i.e., not occurring in either $\mathscr{A}$ or in the $t_i$. The proof is the following sequence. Comments justify, in each case, the presence of the formula immediately to the left by virtue of the presence of the immediately preceding formula:

| | |
|---|---|
| $\mathscr{A}[x_1, x_2]$ | starting point |
| $(\forall x_1)\mathscr{A}[x_1, x_2]$ | generalization |
| $\mathscr{A}[z, x_2]$ | specialization; $x_1 \leftarrow z$ |
| $(\forall x_2)\mathscr{A}[z, x_2]$ | generalization |
| $\mathscr{A}[z, w]$ | specialization; $x_2 \leftarrow w$ |

Now $z \leftarrow t_1$, $w \leftarrow t_2$, *in any order*, is the same as simultaneous substitution I.3.12:

| | |
|---|---|
| $(\forall z)\mathscr{A}[z, w]$ | generalization |
| $\mathscr{A}[t_1, w]$ | specialization; $z \leftarrow t_1$ |
| $(\forall w)\mathscr{A}[t_1, w]$ | generalization |
| $\mathscr{A}[t_1, t_2]$ | specialization; $w \leftarrow t_2$ |

□

**I.4.13 Metatheorem (Variant, or Dummy, Renaming).** *For any formula $(\exists x)\mathscr{A}$, if $z$ does* not *occur in it (i.e., is neither free nor bound), then* $\vdash (\exists x)\mathscr{A} \leftrightarrow (\exists z)\mathscr{A}[x \leftarrow z]$.

We often write this (under the stated conditions) as $\vdash (\exists x)\mathscr{A}[x] \leftrightarrow (\exists z)\mathscr{A}[z]$. By the way, another way to state the conditions is "if $z$ does *not* occur in $\mathscr{A}$ (i.e., is neither free nor bound in $\mathscr{A}$), and is different from $x$". Of course, if $z \equiv x$, then there is nothing to prove.

*Proof.* Since $z$ is substitutable in $x$ under the stated conditions, $\mathscr{A}[x \leftarrow z]$ is defined. Thus, by **Ax2**,

$$\vdash \mathscr{A}[x \leftarrow z] \to (\exists x)\mathscr{A}$$

By $\exists$-introduction – since $z$ is not free in $(\exists x)\mathscr{A}$ – we also have

$$\vdash (\exists z)\mathscr{A}[x \leftarrow z] \to (\exists x)\mathscr{A} \tag{1}$$

We note that $x$ is not free in $(\exists z)\mathscr{A}[x \leftarrow z]$ and is free for $z$ in $\mathscr{A}[x \leftarrow z]$. Indeed, $\mathscr{A}[x \leftarrow z][z \leftarrow x] \equiv \mathscr{A}$. Thus, by **Ax2**,

$$\vdash \mathscr{A} \to (\exists z)\mathscr{A}[x \leftarrow z]$$

Hence, by ∃-introduction

$$\vdash (\exists x)\mathscr{A} \rightarrow (\exists z)\mathscr{A}[x \leftarrow z] \tag{2}$$

Tautological implication from (1) and (2) concludes the argument. □

Why is $\mathscr{A}[x \leftarrow z][z \leftarrow x] \equiv \mathscr{A}$? We can see this by induction on $\mathscr{A}$ (recall that $z$ occurs as neither free nor bound in $\mathscr{A}$).

If $\mathscr{A}$ is atomic, then the claim is trivial. The claim also clearly "propagates" with the propositional formation rules, that is, I.1.8(b).

Consider then the case that $\mathscr{A} \equiv (\exists w)\mathscr{B}$. Note that $w \equiv x$ is possible under our assumptions, but $w \equiv z$ is not. If $w \equiv x$, then $\mathscr{A}[x \leftarrow z] \equiv \mathscr{A}$; in particular, $z$ is not free in $\mathscr{A}$; hence $\mathscr{A}[x \leftarrow z][z \leftarrow x] \equiv \mathscr{A}$ as well.

So let us work with $w \not\equiv x$. By the I.H., $\mathscr{B}[x \leftarrow z][z \leftarrow x] \equiv \mathscr{B}$. Now

$$\begin{aligned}
\mathscr{A}[x \leftarrow z][z \leftarrow x] &\equiv ((\exists w)\mathscr{B})[x \leftarrow z][z \leftarrow x] \\
&\equiv ((\exists w)\mathscr{B}[x \leftarrow z])[z \leftarrow x] && \text{see I.3.11; } w \not\equiv z \\
&\equiv ((\exists w)\mathscr{B}[x \leftarrow z][z \leftarrow x]) && \text{see I.3.11; } w \not\equiv x \\
&\equiv ((\exists w)\mathscr{B}) && \text{I.H.} \\
&\equiv \mathscr{A}
\end{aligned}$$

By I.4.13, the issue of substitutability becomes moot. Since we have an infinite supply of variables (to use, for example, as bound variables), we can always change the names of *all* the bound variables in $\mathscr{A}$ so that the new names are different from all the free variables in $\mathscr{A}$ or $t$. In doing so we obtain a formula $\mathscr{B}$ that is (absolutely) provably equivalent to the original.

Then $\mathscr{B}[x \leftarrow t]$ *will* be defined ($t$ will be substitutable in $x$). Thus, the moral is "any term $t$ is free for $x$ in $\mathscr{A}$ *after an appropriate 'dummy' renaming*".

**I.4.14 Definition.** In the sequel we will often discuss two (or more) theories at once. Let $\mathfrak{T} = (L, \Lambda, \mathbf{I}, \mathscr{T})$ and $\mathfrak{T}' = (L', \Lambda, \mathbf{I}, \mathscr{T}')$ be two theories such that $\mathscr{W} \subseteq \mathscr{W}'$. This enables $\mathfrak{T}'$ to be "aware" of all the formulas of $\mathfrak{T}$ (but *not* vice versa, since $L'$ may contain additional nonlogical symbols – case where $\mathscr{W} \neq \mathscr{W}'$).

We say that $\mathfrak{T}'$ is an *extension* of $\mathfrak{T}$, in symbols $\mathfrak{T} \leq \mathfrak{T}'$, iff $\mathscr{T} \subseteq \mathscr{T}'$.

Let $\mathscr{A}$ be a formula over $L$ (so that both theories are aware of it). The symbols $\vdash_{\mathfrak{T}} \mathscr{A}$ and $\vdash_{\mathfrak{T}'} \mathscr{A}$ are synonymous with $\mathscr{A} \in \mathscr{T}$ and $\mathscr{A} \in \mathscr{T}'$ respectively.

Note that we did not explicitly mention the nonlogical axioms $\Gamma$ or $\Gamma'$ to the left of $\vdash$, since the subscript of $\vdash$ takes care of that information.

We say that the extension is *conservative* iff for any $\mathscr{A}$ over $L$, whenever $\vdash_{\mathfrak{T}'} \mathscr{A}$ it is also the case that $\vdash_{\mathfrak{T}} \mathscr{A}$. That is, when it comes to formulas over the language ($L$) that *both* theories understand, then the new theory does not do any better than the old in producing theorems. □

**I.4.15 Metatheorem (Metatheorem on Constants).** *Let us extend a language $L$ of a theory $\mathfrak{T}$ by adding new constant symbols $e_1, \ldots, e_n$ to the alphabet $\mathscr{V}$, resulting in the alphabet $\mathscr{V}'$, language $L'$, and theory $\mathfrak{T}'$. Furthermore, assume that $\Gamma' = \Gamma$, that is, we did not add any new nonlogical axioms.*

*Then $\vdash_{\mathfrak{T}'} \mathscr{A}[e_1, \ldots, e_n]$ implies $\vdash_{\mathfrak{T}} \mathscr{A}[x_1, \ldots, x_n]$, for any variables $x_1, \ldots, x_n$ that occur nowhere in $\mathscr{A}[e_1, \ldots, e_n]$, as either free or bound variables.*

*Proof.* Fix a set of variables $x_1, \ldots, x_n$ as described above. We do induction on $\mathfrak{T}'$-theorems.

*Basis.* $\mathscr{A}[e_1, \ldots, e_n]$ is a logical axiom (over $L'$); hence so is $\mathscr{A}[x_1, \ldots, x_n]$, *over $L$* – because of the restriction on the $x_i$. Thus $\vdash_{\mathfrak{T}} \mathscr{A}[x_1, \ldots, x_n]$. Note that if $\mathscr{A}[e_1, \ldots, e_n]$ is nonlogical, then so is $\mathscr{A}[x_1, \ldots, x_n]$ under our assumptions.

**Pause.** What does the restriction on the $x_i$ have to do with the claim above?

*Modus ponens.* Here $\vdash_{\mathfrak{T}'} \mathscr{B}[e_1, \ldots, e_n] \to \mathscr{A}[e_1, \ldots, e_n]$ and $\vdash_{\mathfrak{T}'} \mathscr{B}[e_1, \ldots, e_n]$. By I.H., $\vdash_{\mathfrak{T}} \mathscr{B}[y_1, \ldots, y_n] \to \mathscr{A}[y_1, \ldots, y_n]$ and $\vdash_{\mathfrak{T}} \mathscr{B}[y_1, \ldots, y_n]$, where $y_1, \ldots, y_n$ occur nowhere in $\mathscr{B}[e_1, \ldots, e_n] \to \mathscr{A}[e_1, \ldots, e_n]$ as either free or bound variables. By modus ponens, $\vdash_{\mathfrak{T}} \mathscr{A}[y_1, \ldots, y_n]$; hence $\vdash_{\mathfrak{T}} \mathscr{A}[x_1, \ldots, x_n]$ by I.4.12 (and I.4.13).

$\exists$-*introduction.* We have $\vdash_{\mathfrak{T}'} \mathscr{B}[e_1, \ldots, e_n] \to \mathscr{C}[e_1, \ldots, e_n]$, $z$ is not free in $\mathscr{C}[e_1, \ldots, e_n]$, and $\mathscr{A}[e_1, \ldots, e_n] \equiv (\exists z)\mathscr{B}[e_1, \ldots, e_n] \to \mathscr{C}[e_1, \ldots, e_n]$. By the I.H., if $w_1, \ldots, w_n$ – *distinct from $z$* – occur nowhere in $\mathscr{B}[e_1, \ldots, e_n] \to \mathscr{C}[e_1, \ldots, e_n]$ as either free or bound, then we get $\vdash_{\mathfrak{T}} \mathscr{B}[w_1, \ldots, w_n] \to \mathscr{C}[w_1, \ldots, w_n]$. By $\exists$-introduction we get $\vdash_{\mathfrak{T}} (\exists z)\mathscr{B}[w_1, \ldots, w_n] \to \mathscr{C}[w_1, \ldots, w_n]$. By I.4.12 and I.4.13 we get $\vdash_{\mathfrak{T}} (\exists z)\mathscr{B}[x_1, \ldots, x_n] \to \mathscr{C}[x_1, \ldots, x_n]$, i.e., $\vdash_{\mathfrak{T}} \mathscr{A}[x_1, \ldots, x_n]$. □

**I.4.16 Corollary.** *Let us extend a language $L$ of a theory $\mathfrak{T}$ by adding new constant symbols $e_1, \ldots, e_n$ to the alphabet $\mathscr{V}$, resulting in the alphabet $\mathscr{V}'$, language $L'$, and theory $\mathfrak{T}'$. Furthermore, assume that $\Gamma' = \Gamma$, that is, we did not add any new nonlogical axioms.*

*Then $\vdash_{\mathfrak{T}'} \mathscr{A}[e_1, \ldots, e_n]$ iff $\vdash_{\mathfrak{T}} \mathscr{A}[x_1, \ldots, x_n]$ for any choice of variables $x_1, \ldots, x_n$.*

*Proof. If part.* Trivially, $\vdash_{\mathfrak{T}} \mathscr{A}[x_1, \ldots, x_n]$ implies $\vdash_{\mathfrak{T}'} \mathscr{A}[x_1, \ldots, x_n]$; hence $\vdash_{\mathfrak{T}'} \mathscr{A}[e_1, \ldots, e_n]$ by I.4.12.

*Only-if part.* Choose variables $y_1, \ldots, y_n$ that occur nowhere in $\mathscr{A}[e_1, \ldots, e_n]$ as either free or bound. By I.4.15, $\vdash_{\mathfrak{T}} \mathscr{A}[y_1, \ldots, y_n]$; hence, by I.4.12 and I.4.13, $\vdash_{\mathfrak{T}} \mathscr{A}[x_1, \ldots, x_n]$. □

**I.4.17 Remark.** Thus, the extension $\mathfrak{T}'$ of $\mathfrak{T}$ is *conservative*; for, if $\mathscr{A}$ is over $L$, then $\mathscr{A}[e_1, \ldots, e_n] \equiv \mathscr{A}$. Therefore, if $\vdash_{\mathfrak{T}'} \mathscr{A}$, then $\vdash_{\mathfrak{T}'} \mathscr{A}[e_1, \ldots, e_n]$; hence $\vdash_{\mathfrak{T}} \mathscr{A}[x_1, \ldots, x_n]$, that is, $\vdash_{\mathfrak{T}} \mathscr{A}$.

A more emphatic way to put the above is this: $\mathfrak{T}'$ is not aware of any new *nonlogical* facts that $\mathfrak{T}$ did not already know, albeit by a different name. If $\mathfrak{T}'$ can prove $\mathscr{A}[e_1, \ldots, e_n]$, then $\mathfrak{T}$ can prove *the same statement*, using *any* names (other than the $e_i$) that are meaningful in its own language; namely, it can prove $\mathscr{A}[x_1, \ldots, x_n]$. □

The following corollary stems from the proof (rather than the statement) of I.4.15 and I.4.16, and is important.

**I.4.18 Corollary.** *Let $e_1, \ldots, e_n$ be constants that do not appear in the nonlogical axioms $\Gamma$. Then, if $x_1, \ldots, x_n$ are any variables, and if $\Gamma \vdash \mathscr{A}[e_1, \ldots, e_n]$, it is also the case that $\Gamma \vdash \mathscr{A}[x_1, \ldots, x_n]$.*

**I.4.19 Metatheorem (The Deduction Theorem).** *For any closed formula $\mathscr{A}$, arbitrary formula $\mathscr{B}$, and set of formulas $\Gamma$, if $\Gamma + \mathscr{A} \vdash \mathscr{B}$, then $\Gamma \vdash \mathscr{A} \to \mathscr{B}$.*

N.B. $\Gamma + \mathscr{A}$ denotes the augmentation of $\Gamma$ by adding the formula $\mathscr{A}$. In the present metatheorem $\mathscr{A}$ is a single (but unspecified) formula. However, the notation extends to the case where $\mathscr{A}$ is a schema, in which case it means the augmentation of $\Gamma$ by adding all the instances of the schema.

A converse of the metatheorem is also true trivially: That is, $\Gamma \vdash \mathscr{A} \to \mathscr{B}$ implies $\Gamma + \mathscr{A} \vdash \mathscr{B}$. This direction immediately follows by modus ponens and does not require the restriction on $\mathscr{A}$.

*Proof.* The proof is by induction on $\Gamma + \mathscr{A}$-theorems.

*Basis.* Let $\mathscr{B}$ be logical or nonlogical (but, in the latter case, assume $\mathscr{B} \not\equiv \mathscr{A}$). Then $\Gamma \vdash \mathscr{B}$. Since $\mathscr{B} \models_{\textbf{Taut}} \mathscr{A} \to \mathscr{B}$, it follows by I.4.1 that $\Gamma \vdash \mathscr{A} \to \mathscr{B}$.

Now, if $\mathscr{B} \equiv \mathscr{A}$, then $\mathscr{A} \to \mathscr{B}$ is a logical axiom (group **Ax1**); hence $\Gamma \vdash \mathscr{A} \to \mathscr{B}$ once more.

*Modus ponens*. Let $\Gamma + \mathscr{A} \vdash \mathscr{C}$ and $\Gamma + \mathscr{A} \vdash \mathscr{C} \to \mathscr{B}$. By I.H., $\Gamma \vdash \mathscr{A} \to \mathscr{C}$ and $\Gamma \vdash \mathscr{A} \to \mathscr{C} \to \mathscr{B}$. Since $\mathscr{A} \to \mathscr{C}, \mathscr{A} \to \mathscr{C} \to \mathscr{B} \models_{\mathbf{Taut}} \mathscr{A} \to \mathscr{B}$, we have $\Gamma \vdash \mathscr{A} \to \mathscr{B}$.

$\exists$-*introduction.* Let $\Gamma + \mathscr{A} \vdash \mathscr{C} \to \mathscr{D}$ and $\mathscr{B} \equiv (\exists x)\mathscr{C} \to \mathscr{D}$, where $x$ is not free in $\mathscr{D}$. By the I.H., $\Gamma \vdash \mathscr{A} \to \mathscr{C} \to \mathscr{D}$. By I.4.1, $\Gamma \vdash \mathscr{C} \to \mathscr{A} \to \mathscr{D}$; hence $\Gamma \vdash (\exists x)\mathscr{C} \to \mathscr{A} \to \mathscr{D}$ by $\exists$-introduction ($\mathscr{A}$ is closed). One more application of I.4.1 yields $\Gamma \vdash \mathscr{A} \to (\exists x)\mathscr{C} \to \mathscr{D}$. □

**I.4.20 Remark.** (1) Is the restriction that $\mathscr{A}$ must be closed important? Yes. Let $\mathscr{A} \equiv x = a$, where "$a$" is some constant. Then, even though $\mathscr{A} \vdash (\forall x)\mathscr{A}$ by generalization, it is not always true[†] that $\vdash \mathscr{A} \to (\forall x)\mathscr{A}$. This follows from soundness considerations (next section). Intuitively, assuming that our logic "doesn't lie" (that is, it proves no "invalid" formulas), we immediately infer that $x = a \to (\forall x)x = a$ cannot be absolutely provable, for it is a "lie". It fails at least over $\mathbb{N}$, if $a$ is interpreted to be "0".

(2) I.4.16 adds flexibility to applications of the deduction theorem:

$$\vdash_{\mathfrak{T}} (\mathscr{A} \to \mathscr{B})[x_1, \ldots, x_n] \tag{$*$}$$

where $[x_1, \ldots, x_n]$ is the list of all free variables just in $\mathscr{A}$, is equivalent (by I.4.16) to

$$\vdash_{\mathfrak{T}'} (\mathscr{A} \to \mathscr{B})[e_1, \ldots, e_n] \tag{$**$}$$

where $e_1, \ldots, e_n$ are new constants added to $\mathscr{V}$ (with no effect on nonlogical axioms: $\Gamma = \Gamma'$). Now, since $\mathscr{A}[e_1, \ldots, e_n]$ is closed, proving

$$\Gamma' + \mathscr{A}[e_1, \ldots, e_n] \vdash \mathscr{B}[e_1, \ldots, e_n]$$

establishes ($**$), hence also ($*$).

In practice, one does not perform this step explicitly, but ensures that, throughout the $\Gamma + \mathscr{A}$-proof, whatever free variables were present in $\mathscr{A}$ "behaved like constants", or, as we also say, were "frozen".

(3) In some expositions the deduction theorem is *not* constrained by requiring that $\mathscr{A}$ be closed (e.g., Bourbaki (1966b), and more recently Enderton (1972)).

Which version is right? Both are, in their respective contexts. If all the primary rules of inference are "propositional" (e.g., as in Bourbaki (1966b) and Enderton (1972), who only employ modus ponens) – that is, these rules do not meddle with quantifiers – then the deduction theorem is unconstrained. If, on the other hand, full generalization, namely, $\mathscr{A} \vdash (\forall x)\mathscr{A}$, is a permissible rule (primary or derived), then one cannot avoid constraining the application of the

[†] That is, it is not *true in the metatheory* that we can prove $\mathscr{A} \to (\forall x)\mathscr{A}$ *without nonlogical axioms* (absolutely).

deduction theorem, lest one want to derive (the invalid) $\vdash \mathscr{A} \to (\forall x)\mathscr{A}$ from the valid $\mathscr{A} \vdash (\forall x)\mathscr{A}$.

This also entails that approaches such as in Bourbaki (1966b) and Enderton (1972) do *not* derive full generalization. They only allow a weaker rule, "if $\vdash \mathscr{A}$, then $\vdash (\forall x)\mathscr{A}$".[†]

(4) This divergence of approach in choosing rules of inference has some additional repercussions. One has to be careful in defining the semantic counterpart of $\vdash$, namely, $\models$ (see next section). One wants the two symbols to track each other faithfully (Gödel's completeness theorem).[‡] □

**I.4.21 Corollary (Proof by Contradiction).** *Let $\mathscr{A}$ be closed. Then $\Gamma \vdash \mathscr{A}$ iff $\Gamma + \neg\mathscr{A}$ is inconsistent.*

*Proof. If part.* Given that $\mathbf{Thm}_{\Gamma+\neg\mathscr{A}} = \mathbf{Wff}$. In particular, $\Gamma + \neg\mathscr{A} \vdash \mathscr{A}$. By the deduction theorem, $\Gamma \vdash \neg\mathscr{A} \to \mathscr{A}$. But $\neg\mathscr{A} \to \mathscr{A} \models_{\mathbf{Taut}} \mathscr{A}$.

*Only-if part.* Given that $\Gamma \vdash \mathscr{A}$. Hence $\Gamma + \neg\mathscr{A} \vdash \mathscr{A}$ as well (recall I.3.18(2)). Of course, $\Gamma + \neg\mathscr{A} \vdash \neg\mathscr{A}$ too. Since $\mathscr{A}, \neg\mathscr{A} \models_{\mathbf{Taut}} \mathscr{B}$ for an *arbitrary* $\mathscr{B}$, we are done. □

**Pause.** Is it necessary to assume that $\mathscr{A}$ is closed in I.4.21? Why?

The following is important enough to merit stating. It follows from the type of argument we employed in the only-if part above.

**I.4.22 Metatheorem.** *$\mathfrak{T}$ is inconsistent iff for some $\mathscr{A}$, both $\vdash_{\mathfrak{T}} \mathscr{A}$ and $\vdash_{\mathfrak{T}} \neg\mathscr{A}$ hold.*

We also list below a number of quotable proof techniques. These techniques are routinely used by mathematicians, and will be routinely used by us in what follows. The proofs of all the following metatheorems are delegated to the reader.

**I.4.23 Metatheorem (Distributivity or Monotonicity of ∃).** *For any $x$, $\mathscr{A}$, $\mathscr{B}$,*

$$\mathscr{A} \to \mathscr{B} \vdash (\exists x)\mathscr{A} \to (\exists x)\mathscr{B}$$

*Proof.* See Exercise I.11. □

[†] Indeed, they allow a bit more generality, namely, the rule "if $\Gamma \vdash \mathscr{A}$ *with a side condition*, then $\Gamma \vdash (\forall x)\mathscr{A}$. The side condition is that the formulas of $\Gamma$ do not have free occurrences of $x$". Of course, $\Gamma$ can always be taken to be finite (why?), so that this condition is not unrealistic.

[‡] In Mendelson (1987) $\models$ is defined inconsistently with $\vdash$.

**I.4.24 Metatheorem (Distributivity or Monotonicity of ∀).** *For any $x$, $\mathscr{A}$, $\mathscr{B}$,*

$$\mathscr{A} \to \mathscr{B} \vdash (\forall x)\mathscr{A} \to (\forall x)\mathscr{B}$$

*Proof.* See Exercise I.12. □

The term "monotonicity" is inspired by thinking of "→" as "≤". How? Well, we have the tautology

$$(\mathscr{A} \to \mathscr{B}) \leftrightarrow (A \lor B \leftrightarrow B) \qquad (i)$$

If we think of "$\mathscr{A} \lor \mathscr{B}$" as "max($\mathscr{A}$, $\mathscr{B}$)", then the right hand side in $(i)$ above says that $\mathscr{B}$ is the maximum of $\mathscr{A}$ and $\mathscr{B}$. Or that $\mathscr{A}$ is "less than or equal to" $\mathscr{B}$. The above metatheorems say that both ∃ and ∀ preserve this "inequality".

**I.4.25 Metatheorem (The Equivalence Theorem, or Leibniz Rule).** *Let $\Gamma \vdash \mathscr{A} \leftrightarrow \mathscr{B}$, and let $\mathscr{C}'$ be obtained from $\mathscr{C}$ by replacing* some *– possibly, but not necessarily, all – occurrences of a subformula $\mathscr{A}$ of $\mathscr{C}$ by $\mathscr{B}$. Then $\Gamma \vdash \mathscr{C} \leftrightarrow \mathscr{C}'$, i.e.,*

$$\frac{\mathscr{A} \leftrightarrow \mathscr{B}}{\mathscr{C} \leftrightarrow \mathscr{C}'}$$

*is a derived rule.*

*Proof.* The proof is by induction on formulas $\mathscr{C}$. See Exercise I.14. □

Equational or calculational predicate logic is a particular foundation of first order logic that uses the above Leibniz rule as *the* primary rule of inference. In applying such logic one prefers to write proofs as chains of equivalences. Most equivalences in such a chain stem from an application of the rule. See Dijkstra and Scholten (1990), Gries and Schneider (1994), Tourlakis (2000a, 2000b, 2001).

**I.4.26 Metatheorem (Proof by Cases).** *Suppose that $\Gamma \vdash \mathscr{A}_1 \lor \cdots \lor \mathscr{A}_n$, and $\Gamma \vdash \mathscr{A}_i \to \mathscr{B}$ for $i = 1, \ldots, n$. Then $\Gamma \vdash \mathscr{B}$.*

*Proof.* Immediate, by I.4.1. □

Proof by cases usually benefits from the application of the deduction theorem. That is, having established $\Gamma \vdash \mathscr{A}_1 \lor \cdots \lor \mathscr{A}_n$, one then proceeds to adopt, in turn, each $\mathscr{A}_i$ $(i = 1, \ldots, n)$ as a new nonlogical axiom (with its variables "frozen"). In each case ($\mathscr{A}_i$) one proceeds to prove $\mathscr{B}$. At the end of all this one has established $\Gamma \vdash \mathscr{B}$.

In practice we normally use the following *argot*:

"We will consider cases $\mathscr{A}_i$, for $i = 1, \ldots, n$.

**Case** $\mathscr{A}_1$. $\ldots$ therefore, $\mathscr{B}$.[†]

$\ldots$

**Case** $\mathscr{A}_n$. $\ldots$ therefore, $\mathscr{B}$."

**I.4.27 Metatheorem (Proof by Auxiliary Constant).** *Suppose that for formulas $\mathscr{A}$ and $\mathscr{B}$ over the language L we know*

(1) $\Gamma \vdash (\exists x)\mathscr{A}[x]$,

(2) $\Gamma + \mathscr{A}[a] \vdash \mathscr{B}$, *where a is a new constant not in the language L of* $\Gamma$. *Furthermore assume that in the proof of $\mathscr{B}$ all the free variables of $\mathscr{A}[a]$ were frozen.*

*Then* $\Gamma \vdash \mathscr{B}$.

*Proof.* Exercise I.18. □

The technique that flows from this metatheorem is used often in practice. For example, in projective geometry axiomatized as in Veblen and Young (1916), in order to prove Desargues's theorem on perspective triangles on the plane we use some arbitrary point (this is the auxiliary constant) *off* the plane, having verified that the axioms guarantee that such a point exists. It is important to note that Desargues's theorem does not refer to this point at all – hence the term "auxiliary".

**Note.** In this example, from projective geometry, "$\mathscr{B}$" is Desargues's theorem, "$(\exists x)\mathscr{A}[x]$" asserts that there are points outside the plane, $a$ is an arbitrary such point, and the proof (2) starts with words like "Let $a$ be a point off the plane" – which is *argot* for "add the axiom $\mathscr{A}[a]$".

## I.5. Semantics

So what do all these symbols mean? We show in this section how to decode the formal statements (formulas) into informal statements of real mathematics. Conversely, this will entail an understanding of how to code statements of real mathematics in our formal language.

[†] That is, we add the axiom $\mathscr{A}_1$ to $\Gamma$, freezing its variables, and we then prove $\mathscr{B}$.

The rigorous[†] definition of semantics for first order languages is due to Tarski and is often referred to as "Tarski semantics". The flavour of the particular definition given below is that of Shoenfield (1967), and it accurately reflects our syntactic choices – most importantly, the choice to permit "full" generalization $\mathscr{A} \vdash (\forall x)\mathscr{A}$. In particular, we will define the semantic counterpart of $\vdash$, namely, $\models$, pronounced "logically implies", to ensure that $\Gamma \vdash \mathscr{A}$ iff $\Gamma \models \mathscr{A}$. This is the content of Gödel's completeness theorem, which we state without proof in this section (for a proof see, e.g., our volume 1, *Mathematical Logic*).

This section will assume some knowledge of notation and elementary facts from Cantorian (naïve) set theory. We will, among other things, make use of notation such as

$$A^n \qquad (\text{or } \underbrace{A \times \cdots \times A}_{n \text{ times}})$$

for the set of ordered $n$-tuples of members of $A$. We will also use the symbols $\subseteq, \cup, \bigcup_{a \in I}$.[‡]

**I.5.1 Definition.** Given a language $L = (\mathscr{V}, \mathbf{Term}, \mathbf{Wff})$, a *structure* $\mathfrak{M} = (M, \mathscr{I})$ *appropriate for L* is such that $M \neq \emptyset$ is a set (the *domain* or *underlying set* or *universe*[§]) and $\mathscr{I}$ ("$\mathscr{I}$" for *interpretation*) is a mapping that assigns

(1) to each constant $a$ of $\mathscr{V}$ a unique member $a^{\mathscr{I}} \in M$,
(2) to each function $f$ of $\mathscr{V}$ – of arity $n$ – a unique (total)[¶] function $f^{\mathscr{I}} : M^n \to M$,
(3) to each predicate $P$ of $\mathscr{V}$ – of arity $n$ – a unique set $P^{\mathscr{I}} \subseteq M^n$.[#] □

**I.5.2 Remark.** The structure $\mathfrak{M}$ is often written more verbosely, in conformity with practice in algebra. Namely, one unpacks the $\mathscr{I}$ into a list $a^{\mathscr{I}}, b^{\mathscr{I}}, \ldots; f^{\mathscr{I}}, g^{\mathscr{I}}, \ldots; P^{\mathscr{I}}, Q^{\mathscr{I}}, \ldots$ and writes instead $\mathfrak{M} = (M; a^{\mathscr{I}}, b^{\mathscr{I}}, \ldots; f^{\mathscr{I}}, g^{\mathscr{I}}, \ldots;$

[†] One often says "The formal definition of semantics ...", but the word "formal" is misleading here, for we are actually defining semantics in the metatheory (in "real" mathematics), not in some formal theory.

[‡] If we have a set of sets $\{S_a, S_b, S_c, \ldots\}$, where the indices $a, b, c, \ldots$ all come out of an index set $I$, then the symbol $\bigcup_{i \in I} S_i$ stands for the collection of *all* those objects $x$ that are found in *at least one* of the sets $S_i$. It is a common habit to write $\bigcup_{i=0}^{\infty} S_i$ instead of $\bigcup_{i \in \mathbb{N}} S_i$. $A \cup B$ is the same as $\bigcup_{i \in \{1,2\}} S_i$, where we have let $S_1 = A$ and $S_2 = B$.

[§] Often the qualification "of discourse" is added to the terms "domain" and "universe".

[¶] Requiring $f^{\mathscr{I}}$ to be total is a traditional convention. By the way, *total* means that $f^{\mathscr{I}}$ is defined everywhere on $M^n$.

[#] Thus $P^{\mathscr{I}}$ is an $n$-ary relation with inputs and outputs in $M$.

$P^{\mathscr{I}}$, $Q^{\mathscr{I}}$, ... ). Under this understanding, a structure is an underlying set (universe), $M$, along with a *list* of "concrete" constants, functions, and relations that "interpret" corresponding "abstract" items of the language.

Under the latter notational circumstances we often use the symbols $a^{\mathfrak{M}}$, $f^{\mathfrak{M}}$, $P^{\mathfrak{M}}$ (rather than $a^{\mathscr{I}}$, etc.) to indicate the interpretations in $\mathfrak{M}$ of the constant $a$, function $f$, and predicate $P$ respectively.

We have said above "structure *appropriate for $L$*", thus emphasizing the generality of the language and therefore our ability to interpret what we say in it in many different ways.

Often though (e.g., as in formal arithmetic and set theory), we have a structure in mind to begin with, and then build a formal language to formally codify statements about the objects in the structure. Under these circumstances, in effect, we define a language appropriate *for the structure*. We use the symbol $L_{\mathfrak{M}}$ to indicate that the language was built to fit the structure $\mathfrak{M}$. □

**I.5.3 Definition.** We routinely add symbols to a language $L$ (by adding new nonlogical symbols) to obtain a language $L'$. We say that $L'$ is an *extension* of $L$ and that $L$ is a *restriction* of $L'$. Suppose that $\mathfrak{M} = (M, \mathscr{I})$ is a structure for $L$, and let $\mathfrak{M}' = (M, \mathscr{I}')$ be a structure with the same underlying set $M$, but with $\mathscr{I}$ extended to $\mathscr{I}'$ so that the latter gives meaning to all new symbols while it gives the same meaning as $\mathscr{I}$ does to the symbols of $L$.

We call $\mathfrak{M}'$ an *expansion* (rather than extension) of $\mathfrak{M}$, and $\mathfrak{M}$ a *reduct* (rather than restriction) of $\mathfrak{M}'$. We often write $\mathscr{I} = \mathscr{I}' \restriction L$ to indicate that the mapping $\mathscr{I}'$ – restricted to $L$ (symbol "$\restriction$") – equals $\mathscr{I}$. □

**I.5.4 Definition.** Given $L$ and a structure $\mathfrak{M} = (M, \mathscr{I})$ appropriate for $L$. $L(\mathfrak{M})$ denotes the language obtained from $L$ by *adding* to $\mathscr{V}$ a unique new name $\bar{i}$ for *each* object $i \in M$.

This amends the sets **Term**, **Wff** into **Term**($\mathfrak{M}$), **Wff**($\mathfrak{M}$). Members of the latter sets are called $\mathfrak{M}$-terms and $\mathfrak{M}$-formulas respectively.

We extend the mapping $\mathscr{I}$ to the new constants by: $\bar{i}^{\mathscr{I}} = i$ for all $i \in M$ (where the "=" here is metamathematical: equality on $M$). □

All that we have done here is to allow ourselves to do substitutions like $[x \leftarrow i]$ formally. We do instead $[x \leftarrow \bar{i}]$. One next gives "meaning" to *all closed* terms in $L(\mathfrak{M})$. The following uses definition by recursion (I.2.13) and relies on the fact that the rules that define terms are unambiguous.

**I.5.5 Definition.** For *closed* terms $t$ in $\mathbf{Term}(\mathfrak{M})$ we define the symbol $t^{\mathscr{I}} \in M$ inductively:

(1) If $t$ is either $a$ (original constant) or $\bar{i}$ (imported constant), then $t^{\mathscr{I}}$ has already been defined.
(2) If $t$ is the string $ft_1 \ldots t_n$, where $f$ is $n$-ary and $t_1, \ldots, t_n$ are *closed* $\mathfrak{M}$-terms, we define $t^{\mathscr{I}}$ to be the object (of $M$) $f^{\mathscr{I}}(t_1^{\mathscr{I}}, \ldots, t_n^{\mathscr{I}})$. □

Finally, we give meaning to all closed $\mathfrak{M}$-formulas, again by recursion (over **Wff**).

**I.5.6 Definition.** For *any closed* formula $\mathscr{A}$ in $\mathbf{Wff}(\mathfrak{M})$ we define the symbol $\mathscr{A}^{\mathscr{I}}$ inductively. In all cases, $\mathscr{A}^{\mathscr{I}} \in \{\mathbf{t}, \mathbf{f}\}$:

(1) If $\mathscr{A} \equiv t = s$, where $t$ and $s$ are *closed* $\mathfrak{M}$-terms, then $\mathscr{A}^{\mathscr{I}} = \mathbf{t}$ iff $t^{\mathscr{I}} = s^{\mathscr{I}}$. (The last two occurrences of "=" are metamathematical.)
(2) If $\mathscr{A} \equiv Pt_1 \ldots t_n$, where $P$ is an $n$-ary predicate and the $t_i$ are *closed* $\mathfrak{M}$-terms, then $\mathscr{A}^{\mathscr{I}} = \mathbf{t}$ iff $\langle t_1^{\mathscr{I}}, \ldots, t_n^{\mathscr{I}} \rangle \in P^{\mathscr{I}}$ or $P^{\mathscr{I}}(t_1^{\mathscr{I}}, \ldots, t_n^{\mathscr{I}})$ holds. (Or "is true"; see p. 20. Of course, the last occurrence of "=" is metamathematical.)
(3) If $\mathscr{A}$ is any of the *sentences* $\neg\mathscr{B}, \mathscr{B} \vee \mathscr{C}$, then $\mathscr{A}^{\mathscr{I}}$ is determined by the usual truth tables (see p. 31) using the values $\mathscr{B}^{\mathscr{I}}$ and $\mathscr{C}^{\mathscr{I}}$. That is, $(\neg\mathscr{B})^{\mathscr{I}} = F_{\neg}(\mathscr{B}^{\mathscr{I}})$ and $(\mathscr{B} \vee \mathscr{C})^{\mathscr{I}} = F_{\vee}(\mathscr{B}^{\mathscr{I}}, \mathscr{C}^{\mathscr{I}})$. (The last two occurrences of "=" are metamathematical.)
(4) If $\mathscr{A} \equiv (\exists x)\mathscr{B}$, then $\mathscr{A}^{\mathscr{I}} = \mathbf{t}$ iff $(\mathscr{B}[x \leftarrow \bar{i}])^{\mathscr{I}} = \mathbf{t}$ for some $i \in M$. (The last two occurrences of "=" are metamathematical.) □

We have "imported" constants from $M$ into $L$ in order to be able to state the semantics of $(\exists x)\mathscr{B}$ above in the simple manner we just did (following Shoenfield (1967)).

We often state the semantics of $(\exists x)\mathscr{B}$ by writing

$$\big((\exists x)\mathscr{B}[x]\big)^{\mathscr{I}} \text{ is true} \quad \text{iff} \quad (\exists i \in M)(\mathscr{B}[\bar{i}])^{\mathscr{I}} \text{ is true}$$

**I.5.7 Definition.** Let $\mathscr{A} \in \mathbf{Wff}$, and $\mathfrak{M}$ be a structure as above.

An $\mathfrak{M}$-*instance of* $\mathscr{A}$ is an $\mathfrak{M}$-sentence $\mathscr{A}(\overline{i_1}, \ldots, \overline{i_k})$ (that is, all the free variables of $\mathscr{A}$ have been replaced by imported constants).

We say that $\mathscr{A}$ is *valid in* $\mathfrak{M}$, or that $\mathfrak{M}$ is a *model of* $\mathscr{A}$, iff for all $\mathfrak{M}$-instances $\mathscr{A}'$ of $\mathscr{A}$ it is the case that $\mathscr{A}'^{\mathscr{I}} = \mathbf{t}$.[†] Under these circumstances we write $\models_{\mathfrak{M}} \mathscr{A}$.

[†] We henceforth discontinue our pedantic "(The last occurrence of "=" is metamathematical.)".

For any set of formulas $\Gamma$ from **Wff**, $\models_{\mathfrak{M}} \Gamma$, pronounced "$\mathfrak{M}$ *is a model of* $\Gamma$", means that $\models_{\mathfrak{M}} \mathscr{A}$ for all $\mathscr{A} \in \Gamma$.

A formula $\mathscr{A}$ is *universally valid* or *logically valid* (we often say just *valid*) iff every structure appropriate for the language is a model of $\mathscr{A}$.

Under these circumstances we simply write $\models \mathscr{A}$.

If $\Gamma$ is a set of formulas, then we say it is *satisfiable* iff it has a model. It is *finitely satisfiable* iff every finite subset of $\Gamma$ has a model.[†] □

Contrast the concept of *satisfiability* here with that of *propositional* satisfiability (I.3.6). The definition of validity of $\mathscr{A}$ in a structure $\mathfrak{M}$ corresponds with the normal mathematical practice. It says that a formula is true (in a given "context" $\mathfrak{M}$) just in case it is so for all possible values of the free variables.

**I.5.8 Definition.** We say that $\Gamma$ *logically implies* $\mathscr{A}$, in symbols $\Gamma \models \mathscr{A}$, to mean that *every model of* $\Gamma$ *is also a model of* $\mathscr{A}$. □

**I.5.9 Definition (Soundness).** A theory (identified by its nonlogical axioms) $\Gamma$ is *sound* iff, for all $\mathscr{A} \in$ **Wff**, $\Gamma \vdash \mathscr{A}$ implies $\Gamma \models \mathscr{A}$, that is, iff all the theorems of the theory are logically implied by the nonlogical axioms. □

Clearly then, a *pure* theory $\mathfrak{T}$ is sound iff $\vdash_{\mathfrak{T}} \mathscr{A}$ implies $\models \mathscr{A}$ for all $\mathscr{A} \in$ **Wff**. That is, all its theorems are universally valid.

Towards the soundness result[‡] below we look at two tedious (but easy) lemmata.

**I.5.10 Lemma.** *Given a term $t$, variables $x \not\equiv y$, where $y$ does* not occur in *$t$, and a constant $a$. Then, for any term $s$ and formula $\mathscr{A}$, $s[x \leftarrow t][y \leftarrow a] \equiv s[y \leftarrow a][x \leftarrow t]$ and $\mathscr{A}[x \leftarrow t][y \leftarrow a] \equiv \mathscr{A}[y \leftarrow a][x \leftarrow t]$.*

*Proof. Induction on $s$*: Basis:

$$s[x \leftarrow t][y \leftarrow a] \equiv \begin{cases} \text{if } s \equiv x & \text{then } t \\ \text{if } s \equiv y & \text{then } a \\ \text{if } s \equiv z, \text{ where } x \not\equiv z \not\equiv y, & \text{then } z \\ \text{if } s \equiv b & \text{then } b \end{cases}$$
$$\equiv s[y \leftarrow a][x \leftarrow t]$$

[†] These two concepts are often defined just for sentences.

[‡] Also nicknamed "the easy half of Gödel's completeness theorem".

For the induction step let $s \equiv f r_1 \ldots r_n$, where $f$ has arity $n$. Then

$$\begin{aligned} s[x \leftarrow t][y \leftarrow a] &\equiv f r_1[x \leftarrow t][y \leftarrow a] \ldots r_n[x \leftarrow t][y \leftarrow a] \\ &\equiv f r_1[y \leftarrow a][x \leftarrow t] \ldots r_n[y \leftarrow a][x \leftarrow t] \qquad \text{by I.H.} \\ &\equiv s[y \leftarrow a][x \leftarrow t] \end{aligned}$$

*Induction on $\mathscr{A}$*: Basis:

$$\mathscr{A}[x \leftarrow t][y \leftarrow a] \equiv \begin{cases} \text{if } \mathscr{A} \equiv P r_1 \ldots r_n \text{ then} \\ \qquad P r_1[x \leftarrow t][y \leftarrow a] \ldots r_n[x \leftarrow t][y \leftarrow a] \equiv \\ \qquad\quad P r_1[y \leftarrow a][x \leftarrow t] \ldots r_n[y \leftarrow a][x \leftarrow t] \\ \text{if } \mathscr{A} \equiv r = s \text{ then} \\ \qquad r[x \leftarrow t][y \leftarrow a] = s[x \leftarrow t][y \leftarrow a] \equiv \\ \qquad\quad r[y \leftarrow a][x \leftarrow t] = s[y \leftarrow a][x \leftarrow t] \end{cases}$$

$$\equiv \mathscr{A}[y \leftarrow a][x \leftarrow t]$$

The property we are proving, trivially, propagates with Boolean connectives. Let us do the induction step just in the case where $\mathscr{A} \equiv (\exists w)\mathscr{B}$. If $w \equiv x$ or $w \equiv y$, then the result is trivial. Otherwise,

$$\begin{aligned} \mathscr{A}[x \leftarrow t][y \leftarrow a] &\equiv ((\exists w)\mathscr{B})[x \leftarrow t][y \leftarrow a] \\ &\equiv ((\exists w)\mathscr{B}[x \leftarrow t][y \leftarrow a]) \\ &\equiv ((\exists w)\mathscr{B}[y \leftarrow a][x \leftarrow t]) \qquad \text{by I.H.} \\ &\equiv ((\exists w)\mathscr{B})[y \leftarrow a][x \leftarrow t] \\ &\equiv \mathscr{A}[y \leftarrow a][x \leftarrow t] \end{aligned}$$

□

**I.5.11 Lemma.** *Given a structure $\mathfrak{M} = (M, \mathscr{I})$, a term $s$ and a formula $\mathscr{A}$, both over $L(\mathfrak{M})$. Furthermore, each of $s$ and $\mathscr{A}$ have at most one free variable, namely, $x$.*

*Let $t$ be a closed term over $L(\mathfrak{M})$ such that $t^{\mathscr{I}} = i \in M$. Then $(s[x \leftarrow t])^{\mathscr{I}} = (s[x \leftarrow \bar{i}])^{\mathscr{I}}$ and $(\mathscr{A}[x \leftarrow t])^{\mathscr{I}} = (\mathscr{A}[x \leftarrow \bar{i}])^{\mathscr{I}}$. Of course, since $t$ is closed, $\mathscr{A}[x \leftarrow t]$ is defined.*

*Proof. Induction on $s$*: Basis: $s[x \leftarrow t] \equiv s$ if $s \in \{y, a, \bar{j}\}$ $(y \not\equiv x)$. Hence $(s[x \leftarrow t])^{\mathscr{I}} = s^{\mathscr{I}} = (s[x \leftarrow \bar{i}])^{\mathscr{I}}$ in this case. If $s \equiv x$, then $s[x \leftarrow t] \equiv t$ and $s[x \leftarrow \bar{i}] \equiv \bar{i}$, and the claim follows once more.

For the induction step let $s \equiv f r_1 \ldots r_n$, where $f$ has arity $n$. Then

$$\begin{aligned} (s[x \leftarrow t])^{\mathscr{I}} &= f^{\mathscr{I}}\big((r_1[x \leftarrow t])^{\mathscr{I}}, \ldots, (r_n[x \leftarrow t])^{\mathscr{I}}\big) \\ &= f^{\mathscr{I}}\big((r_1[x \leftarrow \bar{i}])^{\mathscr{I}}, \ldots, (r_n[x \leftarrow \bar{i}])^{\mathscr{I}}\big) \qquad \text{by I.H.} \\ &= (s[x \leftarrow \bar{i}])^{\mathscr{I}} \end{aligned}$$

*Induction on $\mathscr{A}$*: Basis: If $\mathscr{A} \equiv Pr_1 \ldots r_n$, then[†]

$$\begin{aligned}(\mathscr{A}[x \leftarrow t])^{\mathscr{I}} &= P^{\mathscr{I}}\big((r_1[x \leftarrow t])^{\mathscr{I}}, \ldots, (r_n[x \leftarrow t])^{\mathscr{I}}\big)\\ &= P^{\mathscr{I}}\big((r_1[x \leftarrow \bar{i}])^{\mathscr{I}}, \ldots, (r_n[x \leftarrow \bar{i}])^{\mathscr{I}}\big)\\ &= (\mathscr{A}[x \leftarrow \bar{i}])^{\mathscr{I}}\end{aligned}$$

Similarly if $\mathscr{A} \equiv r = s$.

The property we are proving, clearly, propagates with Boolean connectives. Let us do the induction step just in the case where $\mathscr{A} = (\exists w)\mathscr{B}$. If $w \equiv x$ the result is trivial. Otherwise, we note that – since $t$ is closed – $w$ does not occur in $t$, and proceed as follows:

$$\begin{aligned}(\mathscr{A}[x \leftarrow t])^{\mathscr{I}} = \mathbf{t} \quad &\text{iff} \quad \big(((\exists w)\mathscr{B})[x \leftarrow t]\big)^{\mathscr{I}} = \mathbf{t}\\ &\text{iff} \quad \big(((\exists w)\mathscr{B}[x \leftarrow t])\big)^{\mathscr{I}} = \mathbf{t}\\ &\text{iff} \quad (\mathscr{B}[x \leftarrow t][w \leftarrow \bar{j}])^{\mathscr{I}} = \mathbf{t} \text{ for some } j \in M, \text{ by I.5.6(4)}\\ &\text{iff} \quad (\mathscr{B}[w \leftarrow \bar{j}][x \leftarrow t])^{\mathscr{I}} = \mathbf{t} \text{ for some } j \in M, \text{ by I.5.10}\\ &\text{iff} \quad \big((\mathscr{B}[w \leftarrow \bar{j}])[x \leftarrow t]\big)^{\mathscr{I}} = \mathbf{t} \text{ for some } j \in M\\ &\text{iff} \quad \big((\mathscr{B}[w \leftarrow \bar{j}])[x \leftarrow \bar{i}]\big)^{\mathscr{I}} = \mathbf{t} \text{ for some } j \in M, \text{ by I.H.}\\ &\text{iff} \quad (\mathscr{B}[w \leftarrow \bar{j}][x \leftarrow \bar{i}])^{\mathscr{I}} = \mathbf{t} \text{ for some } j \in M\\ &\text{iff} \quad (\mathscr{B}[x \leftarrow \bar{i}][w \leftarrow \bar{j}])^{\mathscr{I}} = \mathbf{t} \text{ for some } j \in M, \text{ by I.5.10}\\ &\text{iff} \quad \big(((\exists w)\mathscr{B}[x \leftarrow \bar{i}])\big)^{\mathscr{I}} = \mathbf{t} \text{ by I.5.6(4)}\\ &\text{iff} \quad \big(((\exists w)\mathscr{B})[x \leftarrow \bar{i}]\big)^{\mathscr{I}} = \mathbf{t}\\ &\text{iff} \quad (\mathscr{A}[x \leftarrow \bar{i}])^{\mathscr{I}} = \mathbf{t}\end{aligned}$$

□

**I.5.12 Metatheorem (Soundness).** *Any first order theory (identified by its nonlogical axioms) $\Gamma$, over some language $L$, is sound.*

*Proof.* By induction on $\Gamma$-theorems $\mathscr{A}$, we prove that $\Gamma \models \mathscr{A}$. That is, we fix a structure for $L$, say $\mathfrak{M}$, and assume that $\models_{\mathfrak{M}} \Gamma$. We then proceed to show that $\models_{\mathfrak{M}} \mathscr{A}$.

Basis: If $\mathscr{A}$ is a nonlogical axiom, then our conclusion is part of the assumption, by I.5.7.

If $\mathscr{A}$ is a logical axiom, there are a number of cases:

*Case 1.* $\models_{\mathbf{Taut}} \mathscr{A}$. We fix an $\mathfrak{M}$-instance of $\mathscr{A}$, say $\mathscr{A}'$, and show that $\mathscr{A}'^{\mathscr{I}} = \mathbf{t}$. Let $p_1, \ldots, p_n$ be *all the propositional variables* (alias, *prime formulas*) occurring in $\mathscr{A}'$. Define a valuation $v$ by setting

[†] For a metamathematical relation $Q$, as usual (p. 20), $Q(a, b, \ldots) = \mathbf{t}$, or just $Q(a, b, \ldots)$, stands for $\langle a, b, \ldots \rangle \in Q$.

$v(p_i) = p_i^{\mathscr{I}}$ for $i = 1, \ldots, n$. Clearly, $\mathbf{t} = \bar{v}(\mathscr{A}') = \mathscr{A}'^{\mathscr{I}}$ (the first "=" because $\models_{\mathbf{Taut}} \mathscr{A}'$, the second because after prime formulas have been taken care of, all that remains to be done for the evaluation of $\mathscr{A}'^{\mathscr{I}}$ is to apply Boolean connectives – see I.5.6(3)).

**Pause.** Why is $\models_{\mathbf{Taut}} \mathscr{A}'$?

*Case 2.* $\mathscr{A} \equiv \mathscr{B}[t] \to (\exists x)\mathscr{B}$. Again, we look at an $\mathfrak{M}$-instance $\mathscr{B}'[t'] \to (\exists x)\mathscr{B}'$. We want $(\mathscr{B}'[t'] \to (\exists x)\mathscr{B}')^{\mathscr{I}} = \mathbf{t}$, but suppose instead that

$$(\mathscr{B}'[t'])^{\mathscr{I}} = \mathbf{t} \tag{1}$$

and

$$\big((\exists x)\mathscr{B}'\big)^{\mathscr{I}} = \mathbf{f} \tag{2}$$

Let $t'^{\mathscr{I}} = i$ ($i \in M$). By I.5.11 and (1), $(\mathscr{B}'[\bar{i}])^{\mathscr{I}} = \mathbf{t}$. By I.5.6(4), $\big((\exists x)\mathscr{B}'\big)^{\mathscr{I}} = \mathbf{t}$, contradicting (2).

*Case 3.* $\mathscr{A} \equiv x = x$. Then an arbitrary $\mathfrak{M}$-instance is $\bar{i} = \bar{i}$ for some $i \in M$. By I.5.6(1), $(\bar{i} = \bar{i})^{\mathscr{I}} = \mathbf{t}$.

*Case 4.* $\mathscr{A} \equiv t = s \to (\mathscr{B}[t] \leftrightarrow \mathscr{B}[s])$. Once more, we take an arbitrary $\mathfrak{M}$-instance, $t' = s' \to (\mathscr{B}'[t'] \leftrightarrow \mathscr{B}'[s'])$. Suppose that $(t' = s')^{\mathscr{I}} = \mathbf{t}$. That is, $t'^{\mathscr{I}} = s'^{\mathscr{I}} =$ (let us say) $i$ (in $M$). But then

$$\begin{aligned} (\mathscr{B}'[t'])^{\mathscr{I}} &= (\mathscr{B}'[\bar{i}])^{\mathscr{I}}, &\quad& \text{by I.5.11} \\ &= (\mathscr{B}'[s'])^{\mathscr{I}}, && \text{by I.5.11} \end{aligned}$$

Hence $(\mathscr{B}[t] \leftrightarrow \mathscr{B}[s])^{\mathscr{I}} = \mathbf{t}$.

For the induction step we have two cases:

*Modus ponens.* Let $\mathscr{B}$ and $\mathscr{B} \to \mathscr{A}$ be $\Gamma$-theorems. Fix an $\mathfrak{M}$-instance $\mathscr{B}' \to \mathscr{A}'$. Since $\mathscr{B}', \mathscr{B}' \to \mathscr{A}' \models_{\mathbf{Taut}} \mathscr{A}'$, the argument here is entirely analogous to the case $\mathscr{A} \in \Lambda$ (hence we omit it).

$\exists$-*introduction.* Let $\mathscr{A} \equiv (\exists x)\mathscr{B} \to \mathscr{C}$ and $\Gamma \vdash \mathscr{B} \to \mathscr{C}$, where $x$ is not free in $\mathscr{C}$. By the I.H.

$$\models_{\mathfrak{M}} \mathscr{B} \to \mathscr{C} \tag{3}$$

Let $(\exists x)\mathscr{B}' \to \mathscr{C}'$ be an $\mathfrak{M}$-instance such that (despite expectations) $\big((\exists x)\mathscr{B}'\big)^{\mathscr{I}} = \mathbf{t}$ but

$$\mathscr{C}'^{\mathscr{I}} = \mathbf{f} \tag{4}$$

Thus

$$\mathscr{B}'[\bar{i}]^{\mathscr{I}} = \mathbf{t} \tag{5}$$

for some $i \in M$. Since $x$ is not free in $\mathscr{C}$, $\mathscr{B}'[\bar{i}] \to \mathscr{C}'$ is a false (by (4) and (5)) $\mathfrak{M}$-instance of $\mathscr{B} \to \mathscr{C}$, contradicting (3). □

We have used the condition of $\exists$-introduction above, by saying "Since $x$ is not free in $\mathscr{C}$, $\mathscr{B}'[\bar{i}] \to \mathscr{C}'$ is a[n] . . . $\mathfrak{M}$-instance of $\mathscr{B} \to \mathscr{C}$".

So the condition was useful. But is it essential? Yes, since, for example, if $x \not\equiv y$, then $x = y \to x = y \not\models (\exists x)x = y \to x = y$.

As a corollary of soundness we have the consistency of pure theories:

**I.5.13 Corollary.** *Any first order pure theory is consistent.*

*Proof.* Let $\mathfrak{T}$ be a pure theory over some language $L$. Since $\not\models \neg x = x$, it follows that $\nvdash_{\mathfrak{T}} \neg x = x$, thus $\mathscr{T} \neq \mathbf{Wff}$. □

By $\nvdash \mathscr{A}$ and $\not\models \mathscr{A}$ we mean the metatheoretical statements " '$\vdash \mathscr{A}$' is false" and " '$\models \mathscr{A}$' is false" respectively.

**I.5.14 Corollary.** *Any first order theory that has a model is consistent.*

*Proof.* Let $\mathfrak{T}$ be a first theory over some language $L$, and $\mathfrak{M}$ a model of $\mathfrak{T}$. Since $\not\models_{\mathfrak{M}} \neg x = x$, it follows that $\nvdash_{\mathfrak{T}} \neg x = x$, thus $\mathscr{T} \neq \mathbf{Wff}$. □

*First order definability in a structure.* We are now in a position to make the process of "translation" to and from informal mathematics rigorous.

**I.5.15 Definition.** Let $L$ be a first order language, and $\mathfrak{M}$ a structure for $L$. A *set* (synonymously, *relation*) $S \subseteq M^n$ is *(first order) definable in* $\mathfrak{M}$ *over* $L$ iff for some formula $\mathscr{S}(y_1, \ldots, y_n)$ (see p. 19 for a reminder on round-bracket notation) and for all $i_j$, $j = 1, \ldots, n$, in $M$,

$$\langle i_1, \ldots, i_n \rangle \in S \quad \text{iff} \quad \models_{\mathfrak{M}} \mathscr{S}(\bar{i}_1, \ldots, \bar{i}_n)$$

We often just say "definable in $\mathfrak{M}$".

A function $f : M^n \to M$ is definable in $\mathfrak{M}$ over $L$ iff the relation $y = f(x_1, \ldots, x_n)$ is so definable. □

N.B. Some authors say "(first order) *expressible*" (Smullyan (1992)) rather than "(first order) definable" in a structure.

In the context of $\mathfrak{M}$, the above definition gives precision to statements such as "we code (or translate) an informal statement into the formal language" or "the (formal language) formula $\mathscr{A}$ informally 'says' . . . ", since any (informal) "statement" (or relation) that depends on the informal variables $x_1, \ldots, x_n$ has the form "$\langle x_1, \ldots, x_n \rangle \in S$" for some (informal) set $S$. It also captures the essence of the statement "The (informal) statement $\langle x_1, \ldots, x_n \rangle \in S$ can be written (or can be made) in the formal language."

What "makes" the statement, *in the formal language*, is the formula $\mathscr{S}$.

**I.5.16 Example.** The informal statement "$z$ is a prime" has a formal translation

$$\boldsymbol{S0} < \boldsymbol{z} \wedge (\forall \boldsymbol{x})(\forall \boldsymbol{y})\big(\boldsymbol{z} = \boldsymbol{x} \times \boldsymbol{y} \rightarrow \boldsymbol{x} = \boldsymbol{z} \vee \boldsymbol{x} = \boldsymbol{S0}\big)$$

over the language of elementary number theory, where nonlogical symbols are $\mathbf{0}$, $\boldsymbol{S}$, $+$, $\times$, $<$ and the definition (translation) is effected in the standard structure $\mathfrak{N} = (\mathbb{N}; 0; S, +, \times; <)$, where "$S$" satisfies, for all $n \in \mathbb{N}$, $S(n) = n + 1$ and interprets "$\boldsymbol{S}$" (see I.5.2, p. 54, for the "unpacked" notation we have just used to denote the structure $\mathfrak{N}$). We have used the variable name "$z$" both formally and informally, but we have used a typographical trick: The formal variable was in boldface type while the informal one was in lightface. □

It must be said that translation is not just an art or skill. There are theoretical limitations to translation. The trivial limitation is that if $M$ is an infinite set and, say, $L$ has a finite set of nonlogical symbols (as is the case in arithmetic and set theory), then we cannot define *all* $S \subseteq M$, simply because we do not have enough first order formulas to do so.

There are non-trivial limitations too. Some sets are not first order definable because their definitions are "far too complex" (the reader who wants more on this comment may wish to look up the section on definability and incompletableness in volume 1 of these lectures (*Mathematical Logic*)).

This is a good place to introduce a common notational *argot* that allows us to write mixed-mode formulas that have a formal part (over some language $L$) but may contain informal constants (names, to be sure, but names that have *not* formally been imported into $L$) from some structure $\mathfrak{M}$ appropriate for $L$.

**I.5.17 Informal Definition.** Let $L$ be a first order language, and $\mathfrak{M} = (M, \mathscr{I})$ a structure for $L$. Let $\mathscr{A}$ be a formula with at most $x_1, \ldots, x_n$ free, and $i_1, \ldots, i_n$

be members of $M$. The notation $\mathscr{A}[\![ i_1, \dots, i_n ]\!]$ is an abbreviation of $\big(\mathscr{A}[\overline{i_1}, \dots, \overline{i_n}]\big)^{\mathscr{I}}$. □

This *argot* allows one to substitute informal objects into variables outright, by-passing the procedure of importing formal names for such objects into the language. It is noteworthy that mixed mode formulas can be defined *directly* by induction on formulas – that is, without forming $L(\mathfrak{M})$ first – as follows:

Let $L$ and $\mathfrak{M}$ be as above. Let $x_1, \dots, x_n$ contain all the free variables that appear in a term $t$ or formula $\mathscr{A}$ over $L$ (not over $L(\mathfrak{M})$). Let $i_1, \dots, i_n$ be arbitrary in $M$.

For terms we define

$$t[\![ i_1, \dots i_n ]\!]$$
$$= \begin{cases} i_j & \text{if } t \equiv x_j \ (1 \le j \le n) \\ a^{\mathscr{I}} & \text{if } t \equiv a \\ f^{\mathscr{I}}\big(t_1[\![ i_1, \dots, i_n ]\!], \dots, t_r[\![ i_1, \dots, i_n ]\!]\big) & \text{if } t \equiv f t_1 \dots t_r \end{cases}$$

For formulas we let

$$\mathscr{A}[\![ i_1, \dots i_n ]\!]$$
$$= \begin{cases} t[\![ i_1, \dots i_n ]\!] = s[\![ i_1, \dots i_n ]\!] & \text{if } \mathscr{A} \equiv t = s \\ P\big(t_1[\![ i_1, \dots, i_n ]\!], \dots, t_r[\![ i_1, \dots, i_n ]\!]\big) & \text{if } \mathscr{A} \equiv P t_1 \dots t_r \\ \neg\big(\mathscr{B}[\![ i_1, \dots i_n ]\!]\big) & \text{if } \mathscr{A} \equiv \neg\mathscr{B} \\ \big(\mathscr{B}[\![ i_1, \dots i_n ]\!] \vee \mathscr{C}[\![ i_1, \dots, i_n ]\!]\big) & \text{if } \mathscr{A} \equiv \mathscr{B} \vee \mathscr{C} \\ (\exists a \in M)\mathscr{B}[\![ a, i_1, \dots, i_n ]\!] & \text{if } \mathscr{A} \equiv (\exists z)\mathscr{B}[z, \vec{x}_n] \end{cases}$$

where "$(\exists a \in M)\dots$" is short for "$(\exists a)(a \in M \wedge \dots)$". The right hand side of $=$ has no free (informal) variables, thus it evaluates to **t** or **f**.

We now turn to the "hard half" of Gödel's completeness theorem, which states that our syntactic proof apparatus can faithfully mimic proofs by logical implication. That is, the syntactic apparatus is "complete".

**I.5.18 Definition.** A theory over $L$ (designated by its nonlogical axioms) $\Gamma$ is *semantically complete* iff $\Gamma \models \mathscr{A}$ implies $\Gamma \vdash \mathscr{A}$ for any formula $\mathscr{A}$. □

The term "semantically complete" is not used much. There is a competing *syntactic* notion of completeness, that of *simple completeness*, also called just *completeness*. The latter is the notion one has normally in mind when saying "a *complete* theory", or, in the opposite case, *incomplete*.

The proof of the semantic completeness of every first order theory hinges on the consistency theorem, which we state without proof below.[†] The completeness theorem will then be derived as a corollary.

**I.5.19 Metatheorem (Consistency Theorem).** *If a (first order) theory $\mathcal{T}$ is consistent, then it has a model.*

☡ Metamathematically speaking, a set $S$ is *countable* if it is finite or it can be put in 1-1 correspondence with $\mathbb{N}$. The latter means that there is a total function $f : \mathbb{N} \to S$ that is *onto* – that is, $(\forall x \in S)(\exists n \in \mathbb{N}) f(n) = x$ is true – and 1-1. "1-1" means that $(\forall n \in \mathbb{N})(\forall m \in \mathbb{N})(f(n) = f(m) \to n = m)$ is true.

A set that is not countable is *uncountable*. Cantor has proved that the set of reals, $\mathbb{R}$, is uncountable.

By definition, *a language $L$ is countable or uncountable iff the set of its nonlogical symbols is.*

By definition, *a model is countable or uncountable iff its domain is.* ☡

The technique of proof of I.5.19 yields the following important corollaries.

**I.5.20 Corollary.** *A consistent theory over a countable language has a countable model.*

**I.5.21 Corollary (Löwenheim-Skolem Theorem).** *If a set of formulas $\Gamma$ over a countable language has a model, then it has a countable model.*

**I.5.22 Corollary (Gödel's Completeness Theorem – Hard Half).** *In any countable first order language $L$, $\Gamma \models \mathscr{A}$ implies $\Gamma \vdash \mathscr{A}$.*

*Proof.* Let $\mathscr{B}$ denote the universal closure of $\mathscr{A}$. By Exercise I.21, $\Gamma \models \mathscr{B}$. Thus, $\Gamma + \neg\mathscr{B}$ has no models (why?). Therefore it is inconsistent. Thus, $\Gamma \vdash \mathscr{B}$ (by I.4.21), and hence (specialization), $\Gamma \vdash \mathscr{A}$. □

☡ A way to rephrase completeness is that if $\Gamma \models \mathscr{A}$, then also $\Delta \models \mathscr{A}$, where $\Delta \subseteq \Gamma$ is finite. This follows by soundness, since $\Gamma \models \mathscr{A}$ entails $\Gamma \vdash \mathscr{A}$ and hence $\Delta \vdash \mathscr{A}$, where $\Delta$ consists of just those formulas of $\Gamma$ used in the proof of $\mathscr{A}$. ☡

[†] For a proof see volume 1 of these lectures.

**I.5.23 Corollary (Compactness Theorem).** *In any countable first order language L, a set of formulas* $\Gamma$ *is satisfiable iff it is finitely satisfiable.*

*Proof. Only-if part.* This is trivial, for a model of $\Gamma$ is a model of any finite subset.

*If part.* Suppose that $\Gamma$ is unsatisfiable (it has no models). Then it is inconsistent by the consistency theorem. In particular, $\Gamma \vdash \neg x = x$. Since the pure theory over $L$ is consistent, a $\Gamma$-proof of $\neg x = x$ involves a nonempty finite sequence of nonlogical axioms (formulas of $\Gamma$), $\mathscr{A}_1, \ldots, \mathscr{A}_n$. That is, $\mathscr{A}_1, \ldots, \mathscr{A}_n \vdash \neg x = x$, hence $\{\mathscr{A}_1, \ldots, \mathscr{A}_n\}$ has no model (by soundness). This contradicts the hypothesis. □

Now, if the language $L$ is uncountable, we say that it has *cardinality* $\mathfrak{k}$ if $\mathscr{V}$ (or equivalently, the set of nonlogical symbols) does. Cardinality is studied within ZFC in Chapter VII. However, to extend the consistency theorem and its corollaries to uncountable $L$ one only needs to have an understanding of the informal Cantorian concept and of its basic properties (e.g., the "real" counterpart of VII.5.17) along with a basic (informal) understanding of *ordinals*. The following is true (for a proof outline see volume 1 of these lectures).

**I.5.24 Metatheorem (Consistency Theorem).** *If a (first order) theory* $\mathfrak{T}$ *over a language L of cardinality* $\mathfrak{k}$ *is consistent, then it has a model of cardinality* $\leq \mathfrak{k}$.

**I.5.25 Corollary (Completeness Theorem).** *In any first order language L,* $\Gamma \models \mathscr{A}$ *implies* $\Gamma \vdash \mathscr{A}$.

**I.5.26 Corollary (Gödel-Mal′cev Compactness Theorem).** *In any first order language L, a set of formulas* $\Gamma$ *is satisfiable iff it is finitely satisfiable.*

The Löwenheim-Skolem theorem takes the following form:

**I.5.27 Corollary (Upward Löwenheim-Skolem Theorem).** *If a set of formulas* $\Gamma$ *over a language L of cardinality* $\mathfrak{k}$ *has an infinite model, then it has a model of any cardinality* $\mathfrak{n}$ *such that* $\mathfrak{k} \leq \mathfrak{n}$.

At one extreme, ZFC set theory's intended model is so huge that it is not even a set (its domain, that is, is not). At the other extreme, set theory has only two primary nonlogical symbols; hence, if we believe that it is consistent,[†] it has

[†] We will have an opportunity to explain this hedging later on.

a countable model. Countable models play an important role in the metatheory of ZFC (as we see, e.g., in Chapter VIII).

The (very condensed) material in this ☡☡ passage is not used anywhere in this volume. ☡☡

## I.6. Defined Symbols

We have already mentioned that the language lives, and it is being constantly enriched by new nonlogical symbols through definitions. The reason we do this is to abbreviate undecipherably long formal texts, thus making them humanly understandable.

There are three possible kinds of formal abbreviations, namely, abbreviations of *formulas*, abbreviations of *variable terms* (i.e., objects that depend on free variables), and abbreviations of *constant terms* (i.e., objects that do not depend on free variables). Correspondingly, we introduce a new nonlogical symbol for a *predicate*, a *function*, or a *constant* in order to accomplish such abbreviations.

Here are three simple examples, representative of each case.

We introduce a new *predicate* (symbol), "$\subseteq$", in set theory by a definition[†]

$$A \subseteq B \leftrightarrow (\forall x)(x \in A \rightarrow x \in B)$$

An introduction of a function symbol by definition is familiar from elementary mathematics. There is a theorem that says

$$\begin{array}{l}\text{"for every non-negative real number } x \text{ there is a unique} \\ \text{non-negative real number } y \text{ such that } x = y \cdot y\text{"}\end{array} \tag{1}$$

This justifies the introduction of a 1-ary function symbol $f$ that, for each such $x$, produces the corresponding $y$. Instead of using the generic "$f(x)$", we normally adopt one of the notations "$\sqrt{x}$" or "$x^{1/2}$". Thus, we enrich the language (of, say, algebra) by the function symbol $\sqrt{\ }$ and add as an axiom the definition of its behaviour. This would be

$$x = \sqrt{x}\sqrt{x}$$

or

$$y = \sqrt{x} \leftrightarrow x = y \cdot y$$

where the restriction $x \geq 0$ is implied by the context.

[†] In practice we state the above definition in *argot*, probably as "$A \subseteq B$ means that, for all $x$, we have $x \in A \rightarrow x \in B$".

The “enabling formula” (1) – stated in *argot* above – is crucial in order that we be allowed to introduce $\sqrt{\ }$ and its defining axiom. That is, before we introduce an abbreviation of a (variable or constant) *term* – i.e., an *object* – we must have a proof in our theory of an *existential* formula, i.e., one of the type $(\exists! y)\mathscr{A}$, that asserts that (if applicable, for each “value” of the free variables) a *unique* such object exists.

☡ The symbol “$(\exists! y)$” is read “there is a *unique* $y$”. It is a *logical* abbreviation (defined logical symbol, just like $\forall$) given (in least parenthesized form) by

$$(\exists x)\big(\mathscr{A} \wedge \neg(\exists z)(\mathscr{A} \wedge \neg x = z)\big)$$ ☡

Finally, an example of introducing a new constant symbol, from set theory, is the introduction of the symbol $\emptyset$ into the language, as the name of the unique object[†] $y$ that satisfies $\neg U(y) \wedge (\forall x)x \notin y$, read “$y$ is a set[‡] and it has no members”. Thus, $\emptyset$ is defined by

$$\neg U(\emptyset) \wedge (\forall x)x \notin \emptyset$$

or, equivalently, by

$$y = \emptyset \leftrightarrow \neg U(y) \wedge (\forall x)x \notin y$$

The general situation is this: We start with a theory $\Gamma$, spoken in some *basic*[§] formal language $L$. As the development of $\Gamma$ proceeds, gradually and continuously we *extend* $L$ into languages $L_n$, for $n \geq 0$ (we have set $L_0 = L$). Thus the symbol $L_{n+1}$ stands for some arbitrary extension of $L_n$ effected at *stage* $n + 1$. The theory itself is being extended by stages, as a sequence $\Gamma_n$, $n \geq 0$.

A *stage* is marked by the event of introducing a *single* new symbol into the language via a definition of a new predicate, function, or constant symbol. At that same stage we also add to $\Gamma_n$ the defining nonlogical axiom of the new symbol in question, thus *extending* the theory $\Gamma_n$ into $\Gamma_{n+1}$. We set $\Gamma_0 = \Gamma$.

Specifically, if[¶] $\mathscr{Q}(\vec{x}_n)$ is some formula we then can introduce a new predicate symbol “$P$”[#] that stands for $\mathscr{Q}$.

[†] Uniqueness follows from *extensionality*, while existence follows from *separation*. These facts – and the italicized terminology – are found in Chapter III.

[‡] $U$ is 1-ary (unary) predicate. It is one of the two primitive nonlogical symbols of formal set theory. With the help of this predicate we can test an object for set or atom status. “$U(y)$” asserts that $y$ is an atom; thus “$\neg U(y)$” asserts that $y$ is a set – since we accept that sets or atoms are the only types of objects that the formal system axiomatically characterizes.

[§] “Basic” means here the language given originally, before any new symbols were added.

[¶] Recall that (see Remark I.1.11, p. 19) the notation $\mathscr{Q}(\vec{x}_n)$ asserts that $\vec{x}_n$, i.e., $x_1, \ldots, x_n$ is the *complete* list of the free variables of $\mathscr{Q}$.

[#] Recall that predicate letters are denoted by *non*-calligraphic capital letters $P$, $Q$, $R$ with or without subscripts or primes.

In the present description, $\mathscr{Q}$ is a syntactic (meta-)variable, while $P$ is a new *formal* predicate symbol.

This entails adding $P$ to $L_k$ (i.e., to its alphabet $\mathscr{V}_k$) as a new $n$-ary predicate symbol, and adding

$$P\vec{x}_n \leftrightarrow \mathscr{Q}(\vec{x}_n) \qquad (i)$$

to $\Gamma_k$ as the defining axiom for $P$. "$\subseteq$" is such a defined (2-ary) predicate in set theory.

Similarly, a new $n$-ary function symbol $f$ is added into $L_k$ (to form $L_{k+1}$) by a definition of its behaviour. That is, we add $f$ to $L_k$ and also add the following formula $(ii)$ to $\Gamma_k$ as a new nonlogical axiom

$$y = fy_1 \dots y_n \leftrightarrow \mathscr{Q}(y, y_1, \dots, y_n) \qquad (ii)$$

provided we have a proof in $\Gamma_k$ of the formula

$$(\exists! y)\mathscr{Q}(y, y_1, \dots, y_n). \qquad (iii)$$

Depending on the theory and on the number of free variables ($n \geq 0$), "$f$" may take theory-specific *names* such as $\emptyset$, $\omega$, $\sqrt{\ }$, etc. (in this illustration, for the sake of economy of effort, we have thought of defined constants, e.g., $\emptyset$ and $\omega$, as 0-ary functions).

In effecting these definitions, we want to be assured of two things:

(1) Whatever we can say in the richer language $L_k$ (for any $k > 0$) we can also state in the original (basic) language $L = L_0$ (although awkwardly, which justifies our doing all this). "Can be stated" means that we can translate any formula $\mathscr{F}$ over $L_k$ (hopefully in a "natural" way) into a formula $\mathscr{F}^*$ over $L$ so that the extended theory $\Gamma_k$ can *prove* that $\mathscr{F}$ and $\mathscr{F}^*$ are equivalent.[†]

(2) We also want to be assured that the new symbols offer *no more than convenience*, in the sense that any formula $\mathscr{F}$ *over the basic language* $L$ deducible from $\Gamma_k$ ($k > 0$), one way or another (perhaps with the help of defined symbols) is also deducible from $\Gamma$.[‡]

These assurances will become available shortly, as Metatheorems I.6.1 and I.6.3. Here are the "natural" translation rules that take us from a language stage $L_{k+1}$

[†] $\Gamma$, spoken over $L$, can have no opinion, of course, since it cannot see the new symbols, nor does it have their definitions among its "knowledge".

[‡] Trivially, any $\mathscr{F}$ over $L$ that $\Gamma$ can prove, any $\Gamma_k$ ($k > 0$) can prove as well, since the latter understands the language ($L$) *and* contains all the axioms of $\Gamma$. Thus $\Gamma_k$ extends the theory $\Gamma$. That it cannot have more theorems *over* $L$ than $\Gamma$ makes this extension *conservative*.

back to the previous, $L_k$ (so that, iterating the process, we get back to $L$):

*Rule (1).* Suppose that $\mathscr{F}$ is a formula over $L_{k+1}$, and that the predicate $P$ (whose definition took us from $L_k$ to $L_{k+1}$, and hence is a symbol of $L_{k+1}$ but not of $L_k$) occurs in $\mathscr{F}$ zero or more times. Assume that $P$ has been defined by the axiom $(i)$ above (included in $\Gamma_{k+1}$), where $\mathscr{Q}$ is a formula over $L_k$. We eliminate $P$ from $\mathscr{F}$ by replacing *all its occurrences* by $\mathscr{Q}$. That is, whenever $P\vec{t}_n$ is a subformula of $\mathscr{F}$, all its occurrences are replaced by $\mathscr{Q}(\vec{t}_n)$. We can always arrange by I.4.13 that the simultaneous substitution $\mathscr{Q}[\vec{x}_n \leftarrow \vec{t}_n]$ is defined. This results to a formula $\mathscr{F}^*$ over $L_k$.

*Rule (2).* If $f$ is a defined $n$-ary function symbol as in $(ii)$ above, introduced into $L_{k+1}$, and if it occurs in $\mathscr{F}$ as $\mathscr{F}[ft_1 \ldots t_n]$,[†] then this formula is logically equivalent to[‡]

$$(\exists y)(y = ft_1 \ldots t_n \wedge \mathscr{F}[y]) \tag{$iv$}$$

provided that $y$ is not free in $\mathscr{F}[ft_1 \ldots t_n]$. Using the definition of $f$ given by $(ii)$, and I.4.13 to ensure that $\mathscr{Q}(y, \vec{t}_n)$ is defined, we eliminate this occurrence of $f$, writing $(iv)$ as

$$(\exists y)(\mathscr{Q}(y, t_1, \ldots, t_n) \wedge \mathscr{F}[y]) \tag{$v$}$$

which says the same thing as $(iv)$ in any theory that thinks that $(ii)$ is true (this observation is made precise in the proof of Metatheorem I.6.1). Of course, $f$ may occur many times in $\mathscr{F}$, even "within itself", as in $ffz_1 \ldots z_n y_2 \ldots y_n$,[§] or even in more complicated configurations. Indeed, it may occur within the scope of a quantifier. So the rule becomes: *Apply the transformation taking every atomic subformula $\mathscr{A}[ft_1 \ldots t_n]$ of $\mathscr{F}$ into the form $(v)$ by stages, eliminating at each stage the leftmost-innermost*[¶] *occurrence of $f$ (in the atomic formula we are transforming at this stage), until all occurrences of $f$ are eliminated.* We now have a formula $\mathscr{F}^*$ over $L_k$.

**I.6.1 Metatheorem (Elimination of Defined Symbols I).** *Let $\Gamma$ be any theory over some formal language $L$.*

$(a)$ *Let the formula $\mathscr{Q}$ be over $L$, and $P$ be a new predicate symbol that extends $L$ into $L'$ and $\Gamma$ into $\Gamma'$ via the axiom $P\vec{x}_n \leftrightarrow \mathscr{Q}(\vec{x}_n)$. Then, for any formula*

[†] This notation allows for the possibility that $ft_1 \ldots t_n$ does not occur at all in $\mathscr{F}$ (see the convention on brackets, p. 19).

[‡] See $(C)$ in the proof of Metatheorem I.6.1 below.

[§] Or $f(f(z_1, \ldots, z_n), y_2, \ldots, y_n))$, using brackets and commas to facilitate reading.

[¶] A term $ft_1 \ldots t_n$ is *innermost* iff none of the $t_i$ contains "$f$".

*$\mathscr{F}$ over $L'$, the $P$-elimination as in Rule* (1) *above yields a $\mathscr{F}^*$ over $L$ such that*

$$\Gamma' \vdash \mathscr{F} \leftrightarrow \mathscr{F}^*$$

($b$) *Let $\mathscr{F}[x]$ be over $L$, and let $t$ stand for $f t_1 \ldots t_n$, where $f$ is introduced by* ($ii$) *above as an axiom that extends $\Gamma$ into $\Gamma'$. Assume that no $t_i$ contains the letter $f$ and that $y$ is not free in $\mathscr{F}[t]$. Then*[†]

$$\Gamma' \vdash \mathscr{F}[t] \leftrightarrow (\exists y)(\mathscr{Q}(y, \vec{t}_n) \wedge \mathscr{F}[y])$$

Here "$L'$" is "$L_{k+1}$" (for some $k$) and "$L$" is "$L_k$".

*Proof.* First observe that this metatheorem indeed gives the assurance that, after applying the transformations (1) and (2) to obtain $\mathscr{F}^*$ from $\mathscr{F}$, $\Gamma'$ thinks that the two are equivalent.

($a$): This follows immediately from the Leibniz rule (I.4.25).

($b$): Start with

$$\vdash \mathscr{F}[t] \rightarrow t = t \wedge \mathscr{F}[t] \qquad \text{(by} \vdash t = t \text{ and } \models_{\mathbf{Taut}}\text{-implication)} \qquad (A)$$

Now, by **Ax2**, substitutability, and non-freedom of $y$ in $\mathscr{F}[t]$,

$$\vdash t = t \wedge \mathscr{F}[t] \rightarrow (\exists y)(y = t \wedge \mathscr{F}[y])$$

Hence

$$\vdash \mathscr{F}[t] \rightarrow (\exists y)(y = t \wedge \mathscr{F}[y]) \qquad (B)$$

by ($A$) and $\models_{\mathbf{Taut}}$-implication.[‡]

Conversely,

$$\vdash y = t \rightarrow (\mathscr{F}[y] \leftrightarrow \mathscr{F}[t]) \qquad (\textbf{Ax4}\text{; substitutability was used here})$$

Hence (by $\models_{\mathbf{Taut}}$)

$$\vdash y = t \wedge \mathscr{F}[y] \rightarrow \mathscr{F}[t]$$

Therefore, by $\exists$-introduction (allowed, by our assumption on $y$),

$$\vdash (\exists y)(y = t \wedge \mathscr{F}[y]) \rightarrow \mathscr{F}[t]$$

[†] As we already have remarked, in view of I.4.13, it is unnecessary pedantry to make assumptions on substitutability explicit.

[‡] We will often write just "by $\models_{\mathbf{Taut}}$" meaning to say "by $\models_{\mathbf{Taut}}$-implication".

which, along with $(B)$, establishes

$$\vdash \mathscr{F}[t] \leftrightarrow (\exists y)(y = t \wedge \mathscr{F}[y]) \tag{$C$}$$

Finally, by $(ii)$ (which introduces $\Gamma'$ to the left of $\vdash$), $(C)$, and the Leibniz rule,

$$\Gamma' \vdash \mathscr{F}[t] \leftrightarrow (\exists y)(\mathscr{Q}(y, \vec{t}_n) \wedge \mathscr{F}[y]) \tag{$D$}$$

□

The import of Metatheorem I.6.1 is that if we transform a formula $\mathscr{F}$ – written over some *arbitrary* extension by definitions, $L_{k+1}$, of the basic language $L$ – into a formula $\mathscr{F}^*$ over $L$, then $\Gamma_{k+1}$ (the theory over $L_{k+1}$ that has the benefit of all the added axioms) thinks that $\mathscr{F} \leftrightarrow \mathscr{F}^*$. The reason for this is that we can imagine that we eliminate one new symbol at a time, repeatedly applying the metatheorem above – part (b) to atomic subformulas – forming a sequence of increasingly more basic formulas $\mathscr{F}_{k+1}, \mathscr{F}_k, \mathscr{F}_{k-1}, \ldots, \mathscr{F}_0$, where $\mathscr{F}_0$ is the same string as $\mathscr{F}^*$ and $\mathscr{F}_{k+1}$ is the same string as $\mathscr{F}$.

Now, $\Gamma_{i+1} \vdash \mathscr{F}_{i+1} \leftrightarrow \mathscr{F}_i$ for $i = k, \ldots, 0$, where, if a defined function letter was eliminated at step $i + 1 \to i$, we invoke $(D)$ above and Leibniz rule. Hence, since $\Gamma_0 \subseteq \Gamma_1 \subseteq \cdots \subseteq \Gamma_{k+1}$, we have $\Gamma_{k+1} \vdash \mathscr{F}_{i+1} \leftrightarrow \mathscr{F}_i$ for $i = k, \ldots, 0$, and therefore $\Gamma_{k+1} \vdash \mathscr{F}_{k+1} \leftrightarrow \mathscr{F}_0$.

**I.6.2 Remark (One Point Rule).** The absolutely provable formula in $(C)$ above is sometimes called the *one point rule* (Gries and Schneider (1994), Tourlakis (2000a, 2000b, 2001)). Its "dual"

$$\mathscr{F}[t] \leftrightarrow (\forall y)(y = t \to \mathscr{F}[y])$$

is also given the same nickname and is easily (absolutely) provable using $(C)$ by eliminating $\exists$. □

**I.6.3 Metatheorem (Elimination of Defined Symbols II).** *Let $\Gamma$ be a theory over a language $L$.*

$(a)$ *If $L'$ denotes the extension of $L$ by the new predicate symbol $P$, and $\Gamma'$ denotes the extension of $\Gamma$ by the addition of the axiom $P\vec{x}_n \leftrightarrow \mathscr{Q}(\vec{x}_n)$, where $\mathscr{Q}$ is a formula over $L$, then $\Gamma \vdash \mathscr{F}$ for any formula $\mathscr{F}$ over $L$ such that $\Gamma' \vdash \mathscr{F}$.*

$(b)$ *Assume that*

$$\Gamma \vdash (\exists! y)\mathscr{R}(y, x_1, \ldots, x_n) \tag{$*$}$$

*pursuant to which we defined the* new *function symbol $f$ by the axiom*

$$y = fx_1 \dots x_n \leftrightarrow \mathscr{R}(y, x_1, \dots, x_n) \tag{$**$}$$

*and thus extended $L$ to $L'$ and $\Gamma$ to $\Gamma'$. Then $\Gamma \vdash \mathscr{F}$ for any formula $\mathscr{F}$ over $L$ such that $\Gamma' \vdash \mathscr{F}$.*

*Proof.* This metatheorem assures that extensions of theories by definitions are conservative in that they produce convenience but no additional power (the same old theorems over the original language are the only ones provable).

($a$): By the completeness theorem, we show instead that

$$\Gamma \models \mathscr{F} \tag{1}$$

So let $\mathfrak{M} = (M, \mathscr{I})$ be an arbitrary model of $\Gamma$, i.e., let

$$\models_{\mathfrak{M}} \Gamma \tag{2}$$

We now *expand* the structure $\mathfrak{M}$ into $\mathfrak{M}' = (M, \mathscr{I}')$ – *without adding any new individuals to its domain $M$* – by adding an interpretation, $P^{\mathscr{I}'}$, for the new symbol $P$. We define for every $a_1, \dots, a_n$ in $M$

$$P^{\mathscr{I}'}(a_1, \dots, a_n) = \mathbf{t} \quad \text{iff} \quad \models_{\mathfrak{M}'} \mathscr{Q}(\overline{a}_1, \dots, \overline{a}_n) \quad [\text{i.e., iff} \quad \models_{\mathfrak{M}} \mathscr{Q}(\overline{a}_1, \dots, \overline{a}_n)]$$

Clearly then, $\mathfrak{M}'$ is a model of the new axiom, since, for all $\mathfrak{M}'$-instances of the axiom – such as $P(\overline{a}_1, \dots, \overline{a}_n) \leftrightarrow \mathscr{Q}(\overline{a}_1, \dots, \overline{a}_n)$ – we have

$$\big(P(\overline{a}_1, \dots, \overline{a}_n) \leftrightarrow \mathscr{Q}(\overline{a}_1, \dots, \overline{a}_n)\big)^{\mathscr{I}'} = \mathbf{t}$$

It follows that $\models_{\mathfrak{M}'} \Gamma'$, since we have $\models_{\mathfrak{M}'} \Gamma$, the latter by (2), due to having made no changes to $\mathfrak{M}$ that affect the symbols of $L$. Thus, $\Gamma' \vdash \mathscr{F}$ yields $\models_{\mathfrak{M}'} \mathscr{F}$; hence, since $\mathscr{F}$ is over $L$, $\models_{\mathfrak{M}} \mathscr{F}$. Along with (2), this proves (1).

($b$): As in ($a$), assume (2) in an attempt to prove (1). By ($*$)

$$\models_{\mathfrak{M}} (\exists! y)\mathscr{R}(y, x_1, \dots, x_n)$$

Thus, there is a concrete (i.e., in the metatheory) function $\widehat{f}$ of $n$ arguments that takes its inputs from $M$ and gives its outputs to $M$, the input-output relation being given by (3) below ($\vec{b}_n$ in, $a$ out). To be specific, the semantics of "$\exists!$" implies that for all $b_1, \dots, b_n$ in $M$ there is a *unique* $a \in M$ such that

$$\big(\mathscr{R}(\overline{a}, \overline{b_1}, \dots, \overline{b_n})\big)^{\mathscr{I}} = \mathbf{t} \tag{3}$$

We now expand the structure $\mathfrak{M}$ into $\mathfrak{M}' = (M, \mathscr{T}')$,[†] so that all we add to it is an interpretation for the new function symbol $f$. We let $f^{\mathscr{T}'} = \widehat{f}$. From (2) it follows that

$$\models_{\mathfrak{M}'} \Gamma \tag{2$'$}$$

since we made no changes to $\mathfrak{M}$ other than adding an interpretation of $f$, and since no formula in $\Gamma$ contains $f$. By (3), if $a, b_1, \ldots, b_n$ are any members of $M$, then we have

$$\begin{aligned} \models_{\mathfrak{M}'} \overline{a} = f\overline{b}_1 \ldots \overline{b}_n \quad &\text{iff} \quad a = \widehat{f}(b_1, \ldots, b_n) \\ &\text{iff} \quad \models_{\mathfrak{M}} \mathscr{R}(\overline{a}, \overline{b}_1, \ldots, \overline{b}_n) \qquad \text{by the definition of } \widehat{f} \\ &\text{iff} \quad \models_{\mathfrak{M}'} \mathscr{R}(\overline{a}, \overline{b}_1, \ldots, \overline{b}_n) \end{aligned}$$

– the last “iff” because $\mathscr{R}$ (over $L$) means the same thing in $\mathfrak{M}$ and $\mathfrak{M}'$.

Thus,

$$\models_{\mathfrak{M}'} y = fx_1 \ldots x_n \leftrightarrow \mathscr{R}(y, x_1, \ldots, x_n) \tag{4}$$

Now (∗∗), (2$'$) and (4) yield $\models_{\mathfrak{M}'} \Gamma'$, which implies $\models_{\mathfrak{M}'} \mathscr{F}$ (from $\Gamma' \vdash \mathscr{F}$). Finally, since $\mathscr{F}$ contains no $f$, $\models_{\mathfrak{M}} \mathscr{F}$. This last result and (2) give (1). □

**I.6.4 Remark.**

(a) We note that translation rule (1) and (2) – the latter applied to atomic subformulas – preserve the syntactic structure of quantifier prefixes. For example, suppose that we have introduced $f$ in set theory by

$$y = fx_1 \ldots x_n \leftrightarrow \mathscr{Q}(y, x_1 \ldots, x_n) \tag{5}$$

Now, an application of the *collection* axiom of set theory has a hypothesis of the form

$$\text{“}(\forall x \in Z)(\exists w)(\ldots \mathscr{A}[ft_1 \ldots t_n] \ldots)\text{”} \tag{6}$$

where, say, $\mathscr{A}$ is atomic and the displayed $f$ is innermost. Eliminating this $f$ we have the translation

$$\text{“}(\forall x \in Z)(\exists w)\big(\ldots (\exists y)(\mathscr{A}[y] \wedge \mathscr{Q}(y, t_1, \ldots, t_n)) \ldots\big)\text{”} \tag{7}$$

which still has the $\forall\exists$-prefix and still looks exactly like a collection axiom hypothesis.

(b) Rather than worrying about the ontology of the function *symbol* formally introduced by (5) above – i.e., the question of the exact nature of the symbol

[†] This part is independent of part (a); hence this is a different $\mathscr{T}'$ in general.

that we named "$f$" – in practice we shrug this off and resort to metalinguistic devices to name the function symbol, or the term that naturally arises from it. For example, one can use the notation "$f_{\mathscr{Q}}$" for the function – where the subscript "$\mathscr{Q}$" is the exact string over the language that "$\mathscr{Q}$" denotes – or, for the corresponding term, the notation of Whitehead and Russell (1912),

$$(\iota z)\mathscr{Q}(z, x_1, \ldots, x_n) \tag{8}$$

The "$z$" in (8) above is a bound variable.[†] This new type of term is read "*the* unique $z$ such that . . . ".

This "$\iota$" is *not* one of our primitive symbols.[‡] It is just meant to lead to the friendly shorthand (8) above that avoids the ontology issue.

Thus, once one proves

$$(\exists! z)\mathscr{Q}(z, x_1, \ldots, x_n) \tag{9}$$

one can then introduce (8) by the axiom

$$y = (\iota z)\mathscr{Q}(z, x_1, \ldots, x_n) \leftrightarrow \mathscr{Q}(y, x_1, \ldots, x_n) \tag{5$'$}$$

which, of course, is an alias for axiom (5), using more suggestive notation for the term $f x_1, \ldots, x_n$.

By (9), axioms (5) or (5′) can be replaced by

$$\mathscr{Q}(f x_1, \ldots, x_n, x_1, \ldots, x_n)$$

and

$$\mathscr{Q}((\iota z)\mathscr{Q}(z, x_1, \ldots, x_n), x_1, \ldots, x_n) \tag{10}$$

respectively. For example, from (5′) we get (10) by substitution. Now, **Ax4** (with some help from $\models_{\mathbf{Taut}}$) yields

$$\mathscr{Q}\big((\iota z)\mathscr{Q}(z, x_1, \ldots, x_n),\ x_1, \ldots, x_n\big) \rightarrow \\ y = (\iota z)\mathscr{Q}(z, x_1, \ldots, x_n) \rightarrow \mathscr{Q}(y, x_1, \ldots, x_n)$$

Hence, assuming (10),

$$y = (\iota z)\mathscr{Q}(z, x_1, \ldots, x_n) \rightarrow \mathscr{Q}(y, x_1, \ldots, x_n) \tag{11}$$

[†] That it must be distinct from the $x_i$ is obvious.

[‡] It is however possible to enlarge our alphabet to include "$\iota$", and then add definitions of the syntax of "$\iota$-terms" and axioms for the behaviour of "$\iota$-terms". At the end of all this one gets a *conservative* extension of the original theory, i.e., any $\iota$-free formula provable in the new theory can be also proved in the old (Hilbert and Bernays (1968)).

Finally, deploying (9), we get

$$\mathscr{Q}\big((\iota z)\mathscr{Q}(z, x_1, \ldots, x_n),\ x_1, \ldots, x_n\big) \rightarrow \\ \mathscr{Q}(y, x_1, \ldots, x_n) \rightarrow y = (\iota z)\mathscr{Q}(z, x_1, \ldots, x_n)$$

Hence

$$\mathscr{Q}(y, x_1, \ldots, x_n) \rightarrow y = (\iota z)\mathscr{Q}(z, x_1, \ldots, x_n)$$

by (10). This, along with (11), yields (5′). □ ☡

☡☡ *The indefinite article*. We often have the following situation: We have proved a statement like

$$(\exists x)\mathscr{A}[x] \tag{1}$$

and we want next to derive a statement $\mathscr{B}$.

To this end, we start by picking a symbol $c$ not in $\mathscr{B}$ and say "let $c$ be such that $\mathscr{A}[c]$ is true".[†] That is, we add $\mathscr{A}[c]$ as a nonlogical axiom, treating $c$ as a *new constant*. From all these assumptions we then manage to prove $\mathscr{B}$, hopefully treating all the free variables of $\mathscr{A}[c]$ as constants during the argument. We then conclude that $\mathscr{B}$ has been derived *without the help of* $\mathscr{A}[c]$ *or* $c$ (see I.4.27).

Two things are noteworthy in this technique: One, $c$ does not occur in the conclusion, and, two, $c$ is not uniquely determined by (1). So we have *a* $c$, rather than *the* $c$, that makes $\mathscr{A}[c]$ true.

Now the suggestion that the free variables of the latter be frozen during the derivation of $\mathscr{B}$ is unnecessarily restrictive, and we have a more general result: Suppose that

$$\Gamma \vdash (\exists x)\mathscr{A}(x, y_1, \ldots, y_n) \tag{2}$$

Add a *new* function symbol $f$ to the language $L$ of $\Gamma$ (thus obtaining $L'$) via the axiom

$$\mathscr{A}(f y_1 \ldots y_n, y_1, \ldots, y_n) \tag{3}$$

This says, intuitively, "for any $y_1, \ldots, y_n$, let $x = f y_1 \ldots y_n$ make $\mathscr{A}(x, y_1, \ldots, y_n)$ true". Again, this $x$ is not uniquely determined by (2).

Finally, suppose that we have a proof

$$\Gamma + \mathscr{A}(f y_1 \ldots y_n, y_1, \ldots, y_n) \vdash \mathscr{B} \tag{4}$$

[†] Cf. II.4.1.

such that $f$, the new function symbol, occurs nowhere in $\mathscr{B}$, i.e., the latter formula is over $L$. We can conclude then that

$$\Gamma \vdash \mathscr{B} \tag{5}$$

that is, the extension $\Gamma + \mathscr{A}(fy_1 \ldots y_n, y_1, \ldots, y_n)$ of $\Gamma$ is conservative.

A proof of the legitimacy of this technique, based on the completeness theorem, is easy. Let

$$\models_{\mathfrak{M}} \Gamma \tag{6}$$

and show

$$\models_{\mathfrak{M}} \mathscr{B} \tag{7}$$

Expand the model $\mathfrak{M} = (M, \mathscr{I})$ to $\mathfrak{M}' = (M, \mathscr{I}')$ so that $\mathscr{I}'$ interprets the new symbol $f$. The interpretation is chosen as follows:

(2) guarantees that, for all choices of $i_1, \ldots, i_n$ in $M$, the set $S(i_1, \ldots, i_n) = \{a \in M : \models_{\mathfrak{M}} \mathscr{A}(\overline{a}, \overline{i_1}, \ldots, \overline{i_n})\}$ is not empty. By the axiom of choice (of *informal* set theory), we can pick[†] an $a(i_1, \ldots, i_n)$ in each $S(i_1, \ldots, i_n)$. Thus, we define a function $\widehat{f} : M^n \to M$ by letting, for each $i_1, \ldots, i_n$ in $M$, $\widehat{f}(i_1, \ldots, i_n) = a(i_1, \ldots, i_n)$.

The next step is to set

$$f^{\mathscr{I}'} = \widehat{f}$$

Therefore, for all $i_1, \ldots, i_n$ in $M$,

$$(f\overline{i_1} \ldots \overline{i_n})^{\mathscr{I}'} = \widehat{f}(i_1, \ldots, i_n) = a(i_1, \ldots, i_n)$$

It is now clear that $\models_{\mathfrak{M}'} \mathscr{A}(fy_1 \ldots y_n, y_1, \ldots, y_n)$, for, by I.5.11,

$$(\mathscr{A}(f\overline{i_1} \ldots \overline{i_n}, \overline{i_1}, \ldots, \overline{i_n}))^{\mathscr{I}'} = \mathbf{t} \leftrightarrow (\mathscr{A}(\overline{a(i_1, \ldots, i_n)}, \overline{i_1}, \ldots, \overline{i_n}))^{\mathscr{I}'} = \mathbf{t}$$

and the right hand side of the above is true by the choice of $a(i_1, \ldots, i_n)$.

Thus, $\models_{\mathfrak{M}'} \Gamma + \mathscr{A}(fy_1 \ldots y_n, y_1, \ldots, y_n)$; hence $\models_{\mathfrak{M}'} \mathscr{B}$, by (4).

Since $\mathscr{B}$ contains no $f$, we also have $\models_{\mathfrak{M}} \mathscr{B}$; thus we have established (7) from (6). We now have (5).

One can give a number of names to a function like $f$: A *Skolem function*, an $\varepsilon$-term (Hilbert and Bernays (1968)), or a $\tau$-term (Bourbaki (1966b)). In the first case one may ornament the symbol $f$, e.g., $f_{\exists\mathscr{A}}$, to show where it is coming from, although such mnemonic naming is not, of course, mandatory.

[†] The"$(i_1, \ldots, i_n)$" part indicates that "$a$" depends on $i_1, \ldots, i_n$.

The last two terminologies actually apply to the *term* $f y_1 \dots y_n$, rather than to the function *symbol* $f$.

Hilbert would have written

$$(\varepsilon x)\mathscr{A}(x, y_1 \dots, y_n) \tag{8}$$

and Bourbaki

$$(\tau x)\mathscr{A}(x, y_1 \dots, y_n) \tag{9}$$

each denoting $f y_1 \dots y_n$. The "$x$" in each of (8) and (9) is a bound variable (different from each $y_i$).

## I.7. Formalizing Interpretations

In Section I.5 we discussed Tarski semantics. As we pointed out there (footnote, p. 54), this semantics, while rigorous, is not formal. It is easy to formalize Tarski semantics, and we do so in this section not out of a compulsion to formalize, but because formal interpretations are at the heart of many relative consistency results, some of which we want to discuss in this volume.

As always, we start with a formal language, $L$. We want to interpret its terms and formulas inside some appropriate structure $\mathfrak{M} = (M, \mathscr{I})$. This time, instead of relying on the metatheory to provide us with a universe of discourse, $M$, we will have another formal language[†] $L_i$ and a theory $\mathfrak{T}_i$ over $L_i$ to supply the structure.

Now, such a universe is, intuitively, a collection of individuals. *Any* formula $\mathscr{M}(x)$ over $L_i$ can formally denote a collection of objects. For example, we may think of $\mathscr{M}(x)$ as defining "the collection of all $x$ such that $\mathscr{M}(x)$ holds" (whatever we may intuitively understand by "holds").

We have carefully avoided saying "*set* of all $x$ such that $\mathscr{M}(x)$ holds", since, if (for example) $L_i$ is an extension of the language of set theory, then "the collection of all $x$ such that $x \notin x$ holds" is *not* a set.[‡] Intuitively, such collections are of "enormous size" (this being the reason – again, intuitively – that prevents them from being sets).

The fact that a formula $\mathscr{M}(x)$ might formally denote a collection that is *not* a set is perfectly consistent with our purposes. After all, the intended interpretation of set theory has such a non-set collection as its universe.

[†] The subscript "$i$" is a weak attempt on my part to keep reminding us throughout this section that $L_i$ and $\mathfrak{T}_i$ are to implement an $i$nterpretation of $L$.

[‡] See II.2.1.

The requirement that a universe be nonempty – or that it be true in the metatheory that $M \neq \emptyset$ – translates to the formal requirement that $\mathfrak{T}_i$ can *syntactically*[†] *certify* the nonemptiness:

$$\vdash_{\mathfrak{T}_i} (\exists x)\mathscr{M}(x) \tag{1}$$

The *primary interpretation* mapping, $\mathscr{I}$, is similar to the one defined in I.5.1. We summarize what we have agreed to do so far, "translating" Definition I.5.1 to the one below.

**I.7.1 Definition.** Given a language $L = (\mathscr{V}, \mathbf{Term}, \mathbf{Wff})$.

A *formal interpretation* of $L$ is a 4-tuple $\mathfrak{I} = (L_i, \mathfrak{T}_i, \mathscr{M}(x), \mathscr{I})$, where $L_i = (\mathscr{V}_i, \mathbf{Term}_i, \mathbf{Wff}_i)$ is a first order language (possibly, the same as $L$), $\mathfrak{T}_i$ is a theory over $L_i$, $\mathscr{M}(x)$ is a formula over $L_i$, and $\mathscr{I}$ is a total mapping from the set of nonlogical symbols of $L$ into the set of nonlogical symbols of $L_i$.

Moreover, it is required that the following hold:

(i) (1) above holds.

(ii) For each constant $a$ of $\mathscr{V}$, $a^{\mathscr{I}}$ is a constant of $\mathscr{V}_i$ such that $\vdash_{\mathfrak{T}_i} \mathscr{M}(a^{\mathscr{I}})$.

(iii) For each function $f$ of $\mathscr{V}$, of arity $n$, $f^{\mathscr{I}}$ is function of $\mathscr{V}_i$, of arity $n$, such that

$$\vdash_{\mathfrak{T}_i} \mathscr{M}(x_1) \wedge \mathscr{M}(x_2) \wedge \cdots \wedge \mathscr{M}(x_n) \rightarrow \mathscr{M}(f^{\mathscr{I}} x_1 x_2 \ldots x_n)$$

(iv) For each predicate $P$ of $\mathscr{V}$, $P^{\mathscr{I}}$ is a predicate of $\mathscr{V}_i$, of arity $n$. □

The conditions in I.7.1(ii) and I.7.1(iii) simply say that the universe $\{x : \mathscr{M}\}$ is closed under constants (i.e., contains the interpreting constants, $a^{\mathscr{I}}$) and under the interpreting functions, $f^{\mathscr{I}}$.

Some authors will not assume that $L_i$ *already has* enough nonlogical symbols to effect the mapping $\mathscr{I}$ as plainly as in the definition above. They will instead say that, for example, to any $n$-ary $f$ of $L$, $\mathscr{I}$ will assign a *formula* $\mathscr{A}(y, \vec{x}_n)$ of $L_i$ such that

$$\vdash_{\mathfrak{T}_i} \mathscr{M}(x_1) \wedge \cdots \wedge \mathscr{M}(x_n) \rightarrow (\exists! y)\big(\mathscr{M}(y) \wedge \mathscr{A}(y, \vec{x}_n)\big)$$

In view of our work in the previous section, this would be an unreasonably roundabout way for us to tell the story.

Similarly, the results of Section I.6 allow us, without loss of generality, to always assume that the formula $\mathscr{M}$ in an interpretation $\mathfrak{I} = (\ldots, \mathscr{M}, \ldots)$ is atomic, $Px$, where $P$ is some unary predicate.

[†] We thus substitute the syntactic, or formal, requirement of *provability* for the semantic, or informal, concept of *truth*.

We next formalize the extension of $\mathscr{I}$ to all terms and formulas (cf. I.5.5 and I.5.6).

**I.7.2 Definition.** For every term $t$ over $L$, we define its *relativization* to $\mathscr{M}$, in symbols $t^{\mathscr{M}}$, by induction on $t$:

$$t^{\mathscr{M}} \equiv \begin{cases} a^{\mathscr{I}} & \text{if } t \equiv a \\ z & \text{if } t \equiv z \quad \text{(a variable)} \\ f^{\mathscr{I}} t_1^{\mathscr{M}} \ldots t_n^{\mathscr{M}} & \text{if } t \equiv f t_1 \ldots t_n \end{cases}$$

where $t_1, \ldots, t_n$ are terms over $L$, and $f$ is an $n$-ary function of $L$. □

☡ A trivial induction (on terms $t$ over $L$) proves that $t^{\mathscr{M}}$ is a term over $L_i$. ☡

**I.7.3 Definition.** For every $\mathscr{A}$ over $L$, we define its relativization to $\mathscr{M}$, in symbols $\mathscr{A}^{\mathscr{M}}$, by induction on $\mathscr{A}$:

$$\mathscr{A}^{\mathscr{M}} \equiv \begin{cases} t^{\mathscr{M}} = s^{\mathscr{M}} & \text{if } \mathscr{A} \equiv t = s \\ P^{\mathscr{M}} t_1^{\mathscr{M}} \ldots t_n^{\mathscr{M}} & \text{if } \mathscr{A} \equiv P t_1 \ldots t_n \\ \neg(\mathscr{B}^{\mathscr{M}}) & \text{if } \mathscr{A} \equiv \neg\mathscr{B} \\ (\mathscr{B}^{\mathscr{M}}) \vee (\mathscr{C}^{\mathscr{M}}) & \text{if } \mathscr{A} \equiv \mathscr{B} \vee \mathscr{C} \\ (\exists z)(\mathscr{M}(z) \wedge \mathscr{B}^{\mathscr{M}}) & \text{if } \mathscr{A} \equiv (\exists z)\mathscr{B} \end{cases}$$

where $s, t, t_1, \ldots, t_n$ are terms over $L$, and $P$ is an $n$-ary predicate of $L$. □

☡ The two definitions I.7.2 and I.7.3 are entirely analogous with the definition of *mixed mode* formulas (I.5.17). The analogy stands out if we imagine that "$\mathscr{A}^{\mathscr{M}}$" is some kind of novel notation for "$\mathscr{A}[\![\ldots]\!]$". Particularly telling is the last case (pretend that we have let $M = \{x : \mathscr{M}(x)\}$, where $M$ may or may not be a set).

We have restricted the definition to the primary logical symbols. Thus, e.g., just as $(\forall x)\mathscr{A}$ abbreviates $\neg(\exists x)\neg\mathscr{A}$, we have that $\big((\forall x)\mathscr{A}\big)^{\mathscr{M}}$ abbreviates $\neg\big((\exists x)\neg\mathscr{A}\big)^{\mathscr{M}}$, i.e., $\neg(\exists x)\big(\mathscr{M}(x) \wedge \neg\mathscr{A}^{\mathscr{M}}\big)$, or, in terms of "$\forall$", $(\forall x)\big(\mathscr{M}(x) \to \mathscr{A}^{\mathscr{M}}\big)$.

A trivial induction (on formulas $\mathscr{A}$ over $L$) proves that $\mathscr{A}^{\mathscr{M}}$ is a formula over $L_i$. ☡

We have defined in Section I.5 the symbol $\models_{\mathfrak{M}} \mathscr{A}(x_1, \ldots, x_n)$ to mean

$$\text{For all } a_1, \ldots, a_n \text{ in } M, \mathscr{A}[\![a_1, \ldots, a_n]\!] \text{ is true} \tag{1}$$

Correspondingly, we define the formalization of (1) in $\mathfrak{I}$. Unfortunately, we will use the same symbol as above, $\models$. However, the context will reveal whether it is the semantic or syntactic (formal) version that we are talking about. In the latter case we have a subscript, $\models_{\mathfrak{I}}$, that is a formal interpretation (not a metamathematical structure) name.

**I.7.4 Definition.** Let $\mathfrak{I} = (L_i, \mathfrak{T}_i, \mathscr{M}(x), \mathscr{I})$ be a formal interpretation for a language $L$. For any formula $\mathscr{A}(x_1, \ldots, x_n)$ over $L$, the symbol

$$\models_{\mathfrak{I}} \mathscr{A}(x_1, \ldots, x_n) \tag{2}$$

is short for

$$\vdash_{\mathfrak{T}_i} \mathscr{M}(x_1) \wedge \mathscr{M}(x_2) \wedge \cdots \wedge \mathscr{M}(x_n) \rightarrow \mathscr{A}^{\mathscr{M}}(x_1, \ldots, x_n) \tag{3}$$

The part "$\mathscr{M}(x_1) \wedge \mathscr{M}(x_2) \wedge \cdots \wedge \mathscr{M}(x_n) \rightarrow$" in (3) is empty if $\mathscr{A}$ is a sentence. □

We will (very reluctantly) pronounce (2) above "$\mathscr{A}(x_1, \ldots, x_n)$ is true in the interpretation $\mathfrak{I}$". Even though we have said "true", the context will alert us to the *argot* use of the term, and that we really are talking about provability – (3) – here.

The following lemma is the counterpart of Lemma I.5.11.

**I.7.5 Lemma.** *Given terms $s$ and $t$ and a formula $\mathscr{A}$, all over $L$. Then $(s[x \leftarrow t])^{\mathscr{M}} \equiv s^{\mathscr{M}}[x \leftarrow t^{\mathscr{M}}]$ and $(\mathscr{A}[x \leftarrow t])^{\mathscr{M}} \equiv \mathscr{A}^{\mathscr{M}}[x \leftarrow t^{\mathscr{M}}]$.*

We assume that the operation $[x \leftarrow t]$ is possible, without loss of generality.

*Proof.* The details of the two inductions, on terms $s$ and formulas $\mathscr{A}$, are left to the reader (see the proof of I.5.11).

We only look at one "hard case" in each induction:

*Induction on terms $s$.* Let $s \equiv f t_1 t_2 \ldots t_n$. Then

$$\begin{aligned}
(s[x \leftarrow t])^{\mathscr{M}} &\equiv (f t_1[x \leftarrow t] \ldots t_n[x \leftarrow t])^{\mathscr{M}} \\
&\equiv f^{\mathscr{I}} (t_1[x \leftarrow t])^{\mathscr{M}} \ldots (t_n[x \leftarrow t])^{\mathscr{M}} && \text{by I.7.2} \\
&\equiv f^{\mathscr{I}} t_1^{\mathscr{M}}[x \leftarrow t^{\mathscr{M}}] \ldots t_n^{\mathscr{M}}[x \leftarrow t^{\mathscr{M}}] && \text{by I.H.} \\
&\equiv (f^{\mathscr{I}} t_1^{\mathscr{M}} \ldots t_n^{\mathscr{M}})[x \leftarrow t^{\mathscr{M}}] \\
&\equiv s^{\mathscr{M}}[x \leftarrow t^{\mathscr{M}}] \qquad \text{by I.7.2}
\end{aligned}$$

*Induction on formulas $\mathscr{A}$.* Let $\mathscr{A} \equiv (\exists w)\mathscr{B}$ and $w \not\equiv x$. Then

$$
\begin{aligned}
(\mathscr{A}[x \leftarrow t])^{\mathscr{M}} &\equiv \Big(\big((\exists w)\mathscr{B}\big)[x \leftarrow t]\Big)^{\mathscr{M}} \\
&\equiv \Big((\exists w)\mathscr{B}[x \leftarrow t]\Big)^{\mathscr{M}} \qquad \text{(recall the priority of } [\ldots]) \\
&\equiv (\exists w)\Big(\mathscr{M}(w) \wedge \big(\mathscr{B}[x \leftarrow t]\big)^{\mathscr{M}}\Big) \qquad \text{by I.7.3} \\
&\equiv (\exists w)\Big(\mathscr{M}(w) \wedge \mathscr{B}^{\mathscr{M}}[x \leftarrow t^{\mathscr{M}}]\Big) \qquad \text{by I.H.} \\
&\equiv (\exists w)\big(\mathscr{M}(w) \wedge \mathscr{B}^{\mathscr{M}}\big)[x \leftarrow t^{\mathscr{M}}] \qquad \text{by } w \not\equiv x \\
&\equiv \big((\exists w)\mathscr{B}\big)^{\mathscr{M}}[x \leftarrow t^{\mathscr{M}}], \qquad \text{by I.7.3}
\end{aligned}
$$

□

We will also need the following lemma. It says that all "interpreting objects" are in $\{x : \mathscr{M}\}$.

**I.7.6 Lemma.** *For any term $t$ over $L$,*

$$\vdash_{\mathfrak{T}_i} \mathscr{M}(x_1) \wedge \cdots \wedge \mathscr{M}(x_n) \rightarrow \mathscr{M}\big(t^{\mathscr{M}}[\vec{x}_n]\big) \tag{4}$$

*where all the free variables of $t$ are among the $\vec{x}_n$.*

*Proof.* We have three cases.

(a) $t \equiv a$, a constant. Then the prefix "$\mathscr{M}(x_1) \wedge \cdots \wedge \mathscr{M}(x_n) \rightarrow$" is empty in (4), and the result follows from I.7.1(ii).

(b) $t \equiv z$, a variable. Then (4) becomes $\vdash_{\mathfrak{T}_i} \mathscr{M}(z) \rightarrow \mathscr{M}(z)$.

(c) $t \equiv f t_1 \ldots t_n$. Now (4) is

$$\vdash_{\mathfrak{T}_i} \mathscr{M}(x_1) \wedge \cdots \wedge \mathscr{M}(x_r) \rightarrow \mathscr{M}\big(f^{\mathscr{I}} t_1^{\mathscr{M}}[\vec{x}_r] \ldots t_n^{\mathscr{M}}[\vec{x}_r]\big) \tag{5}$$

To see why (5) holds, freeze the $\vec{x}_r$ and add the axiom $\mathscr{B} \equiv \mathscr{M}(x_1) \wedge \cdots \wedge \mathscr{M}(x_r)$ to $\mathfrak{T}_i$. By the I.H.,

$$\vdash_{\mathfrak{T}_i + \mathscr{B}} \mathscr{M}(t_i^{\mathscr{M}}[\vec{x}_r]) \qquad \text{for } i = 1, \ldots, n$$

By tautological implication, substitution (I.4.12), and I.7.1(iii), the above yields

$$\vdash_{\mathfrak{T}_i + \mathscr{B}} \mathscr{M}\big(f^{\mathscr{I}} t_1^{\mathscr{M}}[\vec{x}_r] \ldots t_n^{\mathscr{M}}[\vec{x}_r]\big)$$

The deduction theorem does the rest. □

We are ready to prove our key result in this connection, namely soundness.

**I.7.7 Theorem.** *Let $\mathfrak{I} = (L_i, \mathfrak{T}_i, \mathscr{M}, \mathscr{T})$ be a formal interpretation of a language L. Then for any $\mathscr{A} \in \Lambda$ over L (cf.* I.3.13*),*

$$\models_{\mathfrak{I}} \mathscr{A}(x_1, \ldots, x_n)$$

*Proof.* We want

$$\vdash_{\mathfrak{T}_i} \mathscr{M}(x_1) \wedge \cdots \wedge \mathscr{M}(x_n) \to \mathscr{A}^{\mathscr{M}}(x_1, \ldots, x_n) \tag{6}$$

for all $\mathscr{A} \in \Lambda$. We have several cases.

**Ax1.** Let $\mathscr{A}(\vec{x}_n)$ be a tautology. As the operation $\ldots^{\mathscr{M}}$ does not change the Boolean connectivity of a formula, so is $\mathscr{A}^{\mathscr{M}}(\vec{x}_n)$. Thus, (6) follows by tautological implication.

**Ax2.** Let $\mathscr{A}(\vec{x}, \vec{y}, \vec{z}) \equiv \mathscr{B}(\vec{x}, t(\vec{x}, \vec{y}), \vec{z}) \to (\exists w)\mathscr{B}(\vec{x}, w, \vec{z})$. By I.7.5,

$$\mathscr{A}^{\mathscr{M}}(\vec{x}, \vec{y}, \vec{z}) \equiv \mathscr{B}^{\mathscr{M}}(\vec{x}, t^{\mathscr{M}}(\vec{x}, \vec{y}), \vec{z}) \to (\exists w)\Big(\mathscr{M}(w) \wedge \mathscr{B}^{\mathscr{M}}(\vec{x}, w, \vec{z})\Big)$$

By I.7.6,

$$\vdash_{\mathfrak{T}_i} \mathscr{M}(x_1) \wedge \cdots \wedge \mathscr{M}(y_1) \wedge \cdots \to \mathscr{M}(t^{\mathscr{M}}(\vec{x}, \vec{y})) \tag{7}$$

Since

$$\mathscr{M}(t^{\mathscr{M}}(\vec{x}, \vec{y})) \wedge \mathscr{B}^{\mathscr{M}}(\vec{x}, t^{\mathscr{M}}(\vec{x}, \vec{y}), \vec{z}) \to (\exists w)\Big(\mathscr{M}(w) \wedge \mathscr{B}^{\mathscr{M}}(\vec{x}, w, \vec{z})\Big)$$

is in $\Lambda$ over $L_i$, (7) and tautological implication yield

$$\begin{aligned}\vdash_{\mathfrak{T}_i} \mathscr{M}(x_1) \wedge \cdots \wedge \mathscr{M}(y_1) \wedge \cdots \to& \\ \mathscr{B}^{\mathscr{M}}(\vec{x}, t^{\mathscr{M}}(\vec{x}, \vec{y}), \vec{z}) \to (\exists w)&\Big(\mathscr{M}(w) \wedge \mathscr{B}^{\mathscr{M}}(\vec{x}, w, \vec{z})\Big)\end{aligned}$$

One more tautological implication gives what we want:

$$\vdash_{\mathfrak{T}_i} \mathscr{M}(x_1) \wedge \cdots \wedge \mathscr{M}(y_1) \wedge \cdots \wedge \mathscr{M}(z_1) \wedge \cdots \to \mathscr{A}^{\mathscr{M}}(\vec{x}, \vec{y}, \vec{z})$$

**Ax3.** Let $\mathscr{A}(x) \equiv x = x$. We want $\vdash_{\mathfrak{T}_i} \mathscr{M}(x) \to x = x$, which holds by tautological implication and the fact that $x = x$ is logical over $L_i$.

**Ax4.** Here $\mathscr{A}[\vec{x}_n] \equiv t = s \to (\mathscr{B}[x \leftarrow t] \leftrightarrow \mathscr{B}[x \leftarrow s])$, where $\vec{x}_n$ includes all the participating free variables. Thus, using I.7.5, (6) translates into

$$\begin{aligned}\vdash_{\mathfrak{T}_i} \mathscr{M}(x_1) \wedge \cdots \wedge \mathscr{M}(x_n) \to t^{\mathscr{M}} = s^{\mathscr{M}}& \\ \to (\mathscr{B}^{\mathscr{M}}[x \leftarrow t^{\mathscr{M}}] \leftrightarrow \mathscr{B}^{\mathscr{M}}[x \leftarrow s^{\mathscr{M}}])&\end{aligned}$$

which holds by tautological implication from the instance of the Leibniz axiom over $L_i$, $t^{\mathscr{M}} = s^{\mathscr{M}} \to (\mathscr{B}^{\mathscr{M}}[x \leftarrow t^{\mathscr{M}}] \leftrightarrow \mathscr{B}^{\mathscr{M}}[x \leftarrow s^{\mathscr{M}}])$. □

I have used above abbreviations such as "$\mathscr{B}^{\mathscr{M}} \to \mathscr{A}^{\mathscr{M}}$" for the abbreviation "$(\mathscr{B} \to \mathscr{A})^{\mathscr{M}}$", etc.

We next direct our attention to some theory $\mathfrak{T}$ over $L$.

**I.7.8 Definition.** Let $\mathfrak{T}$ be a theory over $L$ and $\mathfrak{I} = (L_i, \mathfrak{T}_i, \mathscr{M}, \mathscr{T})$ be a formal interpretation of $L$ over the language $L_i$.

We say that $\mathfrak{I}$ is a *formal interpretation of the theory* (or a *formal model of the theory*) $\mathfrak{T}$ just in case, for every *nonlogical axiom* $\mathscr{A}$ of $\mathfrak{T}$, it is $\models_{\mathfrak{I}} \mathscr{A}$ (cf. I.7.4). □

**I.7.9 Theorem (Formal Soundness).** *If $\mathfrak{I} = (L_i, \mathfrak{T}_i, \mathscr{M}, \mathscr{T})$ is a formal interpretation of the theory $\mathfrak{T}$ over L, then, for any formula $\mathscr{A}$ over L, $\vdash_{\mathfrak{T}} \mathscr{A}$ implies $\models_{\mathfrak{I}} \mathscr{A}$.* □

*Proof.* We do induction on $\mathfrak{T}$-theorems. For the basis, if $\mathscr{A}$ is logical, then we are done by I.7.7. If it is nonlogical, then we are done by definition (I.7.8).

Assume then that $\vdash_{\mathfrak{T}} \mathscr{B} \to \mathscr{A}$ and $\vdash_{\mathfrak{T}} \mathscr{B}$, and let $\vec{x}_n$ include all the free variables of these two formulas. By the I.H.,

$$\vdash_{\mathfrak{T}_i} \mathscr{M}(x_1) \wedge \cdots \wedge \mathscr{M}(x_n) \to \mathscr{B}^{\mathscr{M}} \to \mathscr{A}^{\mathscr{M}}$$

and

$$\vdash_{\mathfrak{T}_i} \mathscr{M}(x_1) \wedge \cdots \wedge \mathscr{M}(x_n) \to \mathscr{B}^{\mathscr{M}}$$

The above two and tautological implication yield

$$\vdash_{\mathfrak{T}_i} \mathscr{M}(x_1) \wedge \cdots \wedge \mathscr{M}(x_n) \to \mathscr{A}^{\mathscr{M}}$$

Finally, let it be the case that $\mathscr{A} \equiv (\exists z)\mathscr{B} \to \mathscr{C}$, where $z$ is not free in $\mathscr{C}$, and moreover $\vdash_{\mathfrak{T}} \mathscr{B} \to \mathscr{C}$. Let $z, \vec{x}_n$ – distinct variables – include all the free variables of $\mathscr{B} \to \mathscr{C}$.

By the I.H.,

$$\vdash_{\mathfrak{T}_i} \mathscr{M}(z) \wedge \mathscr{M}(x_1) \wedge \cdots \wedge \mathscr{M}(x_n) \to \mathscr{B}^{\mathscr{M}} \to \mathscr{C}^{\mathscr{M}}$$

Hence (by tautological implication)

$$\vdash_{\mathfrak{T}_i} \mathscr{M}(z) \wedge \mathscr{B}^{\mathscr{M}} \to \mathscr{M}(x_1) \to \cdots \to \mathscr{M}(x_n) \to \mathscr{C}^{\mathscr{M}}$$

By $\exists$-introduction,

$$\vdash_{\mathfrak{T}_i} (\exists z)\big(\mathscr{M}(z) \wedge \mathscr{B}^{\mathscr{M}}\big) \to \mathscr{M}(x_1) \to \cdots \to \mathscr{M}(x_n) \to \mathscr{C}^{\mathscr{M}}$$

Utilizing tautological implication again, and Definition I.7.3, we are done:

$$\vdash_{\mathfrak{T}_i} \mathscr{M}(x_1) \wedge \cdots \wedge \mathscr{M}(x_n) \to \big((\exists z)\mathscr{B}\big)^{\mathscr{M}} \to \mathscr{C}^{\mathscr{M}}$$ □

It is a shame to call the next result just a “corollary”, for it is *the* result on which we will base the various relative consistency results in this volume (with the sole exception of those in Chapter VIII, where we work in the metatheory, mostly).

The corollary simply says that if the theory, $\mathfrak{T}_i$, in which we interpret $\mathfrak{T}$ is not "broken", then $\mathfrak{T}$ is consistent. This is the formal counterpart of the easy half of Gödel's completeness theorem: If a theory $\mathfrak{T}$ has a (metamathematical) model,[†] then it is consistent.

**I.7.10 Corollary.** *Let $\mathfrak{I} = (L_i, \mathfrak{T}_i, \mathscr{M}, \mathscr{I})$ be a formal model of the theory $\mathfrak{T}$ over L. If $\mathfrak{T}_i$ is consistent, then so is $\mathfrak{T}$.*

*Proof.* We prove the contrapositive. Let $\mathfrak{T}$ be inconsistent; thus

$$\vdash_{\mathfrak{T}} \neg x = x$$

By I.7.9, $\vdash_{\mathfrak{T}_i} \mathscr{M}(x) \to \neg x = x$; thus, by I.4.23,

$$\vdash_{\mathfrak{T}_i} (\exists x)\mathscr{M}(x) \to (\exists x)\neg x = x$$

Since $\vdash_{\mathfrak{T}_i} (\exists x)\mathscr{M}(x)$ by I.7.1, modus ponens yields $\vdash_{\mathfrak{T}_i} (\exists x)\neg x = x$, which along with $\vdash_{\mathfrak{T}_i} (\forall x)x = x$ shows that $\mathfrak{T}_i$ is inconsistent. □

We conclude the section with a brief discussion of a formal version of structure isomorphisms. In the case of "real structures" $\mathfrak{M} = (M, \ldots)$ and $\mathfrak{N} = (N, \ldots)$, we have shown in volume 1 that if $\phi : M \to N$ is a 1-1 correspondence that preserves the meaning of all basic symbols, then it preserves the meaning of everything, that is, if $\mathscr{A}$ is a formula and $a, b, \ldots$ are in $M$, then $\models_{\mathfrak{M}} \mathscr{A}[\![ a, b, \ldots ]\!]$ iff $\models_{\mathfrak{N}} \mathscr{A}[\![ \phi(a), \phi(b), \ldots ]\!]$.

We will use the formal version only once in this volume; thus we feel free to restrict it to our purposes. To begin with, we assume a language $L$ whose only nonlogical symbols are a unary and a binary predicate, which we will denote by $U$ and $\in$ respectively (we have set theory in mind, of course). The interpretations of $L$ whose isomorphisms we want to define and discuss are $\mathfrak{I} = (L_i, \mathfrak{T}_i, \mathscr{M}, \mathscr{I})$ and $\mathfrak{J} = (L_i, \mathfrak{T}_i, \mathscr{N}, \mathscr{J})$. Note that $\mathfrak{T}_i$ and $L_i$ are the same in both interpretations.

Let now $\phi$ be a unary function symbol in $L_i$. It is a *formal isomorphism* of the two interpretations iff the following hold:

(1) $\vdash_{\mathfrak{T}_i} \mathscr{N}(x) \to (\exists y)\big(\mathscr{M}(y) \land x = \phi(y)\big)$ ("ontoness")
(2) $\vdash_{\mathfrak{T}_i} \mathscr{M}(x) \land \mathscr{M}(y) \to \big(x = y \leftrightarrow \phi(x) = \phi(y)\big)$ ("1-1ness"[‡])

[†] It is a well-established habit not to doubt the metatheory's reliability, a habit that has had its critics, including Hilbert, whose metatheory sought "reliability" in simplicity. But we are not getting into that discussion again.

[‡] The → half of ↔ we get for free by an application of the Leibniz axiom.

(3) $\vdash_{\mathfrak{T}_i} \mathscr{M}(x) \to \big(U^{\mathscr{M}}(x) \leftrightarrow U^{\mathscr{N}}(\phi(x)\big)$ ("preservation of $U$"†)
(4) $\vdash_{\mathfrak{T}_i} \mathscr{M}(x) \wedge \mathscr{M}(y) \to \big(x \in^{\mathscr{M}} y \leftrightarrow \phi(x) \in^{\mathscr{N}} \phi(y)\big)$ ("preservation of $\in$")

If $L$ contains a constant $c$, then we must also have $\phi(c^{\mathscr{M}}) = c^{\mathscr{N}}$. This is met in our only application later on by having $c^{\mathscr{M}} = c = c^{\mathscr{N}}$ and $\phi(c) = c$.

**I.7.11 Remark.** In what follows we will present quite a number of formal proofs. It is advisable then at this point to offer a proof-writing tool that will, hopefully, shorten many of these proofs.

Whenever the mathematician is aware (of proofs) of a chain of equivalences such as

$$\mathscr{A}_1 \leftrightarrow A_2, \qquad \mathscr{A}_2 \leftrightarrow A_3, \qquad \mathscr{A}_3 \leftrightarrow A_4, \ldots, \qquad \mathscr{A}_{n-1} \leftrightarrow A_n$$

he often writes instead

$$\mathscr{A}_1 \leftrightarrow A_2 \leftrightarrow A_3 \leftrightarrow A_4 \leftrightarrow \cdots \leftrightarrow \mathscr{A}_{n-1} \leftrightarrow A_n$$

i.e., abusing notation and treating "↔" *conjunctionally* rather than (the correct) *associatively*. This parallels the (ab)uses

$$a < b < c \qquad \text{for} \quad a < b \text{ and } b < c$$

and

$$a = b = c \qquad \text{for} \quad a = b \text{ and } b = c$$

Of course, such a chain also proves $\mathscr{A}_1 \leftrightarrow A_n$ by tautological equivalence.

Moreover, $\mathscr{A}_1$ is provable iff $\mathscr{A}_n$ is (by tautological implication).

More generally, the chain may involve a mix of "↔" and "→". Again tautological equivalence yields a proof of $\mathscr{A}_1 \to \mathscr{A}_n$ this time.

Dijkstra and Scholten (1990), Gries and Schneider (1994), and Tourlakis (2000a, 2000b, 2001) suggest a vertical layout of such chains and say that such a chain constitutes a *calculational proof*:

$$\begin{array}{ll}
& \mathscr{A}_1 \\
\leftrightarrow & \text{or } \to \Big\langle \text{annotation/reason} \Big\rangle \\
& \mathscr{A}_2 \\
\leftrightarrow & \text{or } \to \Big\langle \text{annotation/reason} \Big\rangle \\
& \vdots \\
\leftrightarrow & \text{or } \to \Big\langle \text{annotation/reason} \Big\rangle \\
& \mathscr{A}_n
\end{array}$$

† We write "$U^{\mathscr{M}}$" rather than "$U^{\mathscr{T}}$", as this will be the habitual notation in the context of set theory.

from which

$$\vdash_{\mathscr{T}} \mathscr{A}_1 \to \mathscr{A}_n$$

follows, where $\mathscr{T}$ is the theory within which we reasoned above.

Moreover, if $\vdash_{\mathscr{T}} \mathscr{A}_1$, then also $\vdash_{\mathscr{T}} \mathscr{A}_n$ by modus ponens. □

We can now prove:

**I.7.12 Lemma.** *Let L be a language with just U and* $\in$, *above, as its nonlogical symbols, and let* $\phi$ *be a formal isomorphism of its two interpretations* $\mathfrak{I} = (L_i, \mathfrak{T}_i, \mathscr{M}, \mathscr{T})$ *and* $\mathfrak{J} = (L_i, \mathfrak{T}_i, \mathscr{N}, \mathscr{J})$ *in the sense of* (1)–(4). *Then, for every formula* $\mathscr{A}(\vec{x}_n)$ *over L,*

$$\vdash_{\mathfrak{T}_i} \mathscr{M}(x_1) \wedge \cdots \wedge \mathscr{M}(x_n) \to \big(\mathscr{A}^{\mathscr{M}}(\vec{x}_n) \leftrightarrow \mathscr{A}^{\mathscr{N}}(\phi(x_1), \ldots, \phi(x_n))\big)$$

*Proof.* Induction on formulas. For the atomic ones the statement is just (2)–(4) above. We skip the trivial $\vee$ and $\neg$ cases and look into $\mathscr{A}(\vec{x}_n) \equiv (\exists y)\mathscr{B}(y, \vec{x}_n)$. First,

$$\mathscr{A}^{\mathscr{M}}(\vec{x}_n) \equiv (\exists y)\big(\mathscr{M}(y) \wedge \mathscr{B}^{\mathscr{M}}(y, \vec{x}_n)\big) \tag{5}$$

and

$$\mathscr{A}^{\mathscr{N}}(\phi(x_1), \ldots, \phi(x_n)) \equiv (\exists y)\big(\mathscr{N}(y) \wedge \mathscr{B}^{\mathscr{N}}(y, \phi(x_1), \ldots, \phi(x_n))\big) \tag{6}$$

We now freeze the $\vec{x}_n$ and work in $\mathfrak{T}_i + \mathscr{M}(x_1) \wedge \cdots \wedge \mathscr{M}(x_n)$. We calculate as follows:

$$\begin{aligned}
& (\exists y)\big(\mathscr{N}(y) \wedge \mathscr{B}^{\mathscr{N}}(y, \phi(x_1), \ldots, \phi(x_n))\big) \\
\leftrightarrow\ & \big\langle \text{by (1) and Leibniz rule; } z \text{ a new variable} \big\rangle \\
& (\exists y)\Big((\exists z)\big(\mathscr{M}(z) \wedge y = \phi(z)\big) \wedge \mathscr{B}^{\mathscr{N}}(y, \phi(x_1), \ldots, \phi(x_n))\Big) \\
\leftrightarrow\ & \big\langle \text{newness of } z \big\rangle \\
& (\exists z)(\exists y)\big(\mathscr{M}(z) \wedge y = \phi(z) \wedge \mathscr{B}^{\mathscr{N}}(y, \phi(x_1), \ldots, \phi(x_n))\big) \\
\leftrightarrow\ & \big\langle \text{one point rule (I.6.2) and Leibniz rule} \big\rangle \\
& (\exists z)\big(\mathscr{M}(z) \wedge \mathscr{B}^{\mathscr{N}}(\phi(z), \phi(x_1), \ldots, \phi(x_n))\big) \\
\leftrightarrow\ & \big\langle \text{I.H. and Leibniz rule} \big\rangle \\
& (\exists z)\big(\mathscr{M}(z) \wedge \mathscr{B}^{\mathscr{M}}(z, \vec{x}_n)\big)
\end{aligned}$$

The top line of our calculation is (6), while the bottom is (5) (within bound variable renaming); thus we are done by the deduction theorem. □

## I.8. The Incompleteness Theorems

This brief section is only meant to acquaint the reader with what Gödel's incompleteness theorems are about. The second theorem in particular is one that we will invoke a number of times in this volume; therefore it is desirable to present here the statements of these two theorems and outline, at the intuitive level, what makes them tick. A full exposition and complete proofs for both theorems can be found in our companion volume *Mathematical Logic*.

Now, Gödel's *completeness* theorem asserts the adequacy of the syntactic proof apparatus for characterization of "truth". On the other hand, his *incompleteness theorems* assert the *inadequacy* of this syntactic apparatus for capturing "truth". The contradiction is only apparent. Completeness says that *truth of a formula in all concrete worlds* (all models) of a first order theory *can* be adequately captured – the formula is provable. Incompleteness addresses truth in *one* world. Often such a world is *the* one that matters: The *intended* or *natural* model of a theory that we want to study axiomatically. A formula of the theory that is true (in the Tarski semantics sense) in the intended model is, naturally, called *really true*. An example of such a special world is our familiar structure, $\mathfrak{N} = (\mathbb{N}; S, +, \times; <; 0)$. *Peano arithmetic* is the associated formal theory that attempts to characterize this structure.

The *first incompleteness theorem* in its semantic version says that Peano arithmetic, or indeed *any* reasonably well-constructed extension, cannot do a very good job of proving all the formulas that are really true (in $\mathfrak{N}$). It misses infinitely many. Hence the term "incompleteness", or, more emphatically, "incompletableness", the latter because we cannot make incompleteness go away by throwing axioms at it.

Let us dispense with some terminology before we can actually state and discuss the theorems.

**I.8.1 Definition.** The language for Peano arithmetic we denote by $L_{\mathfrak{N}}$. It has the nonlogical symbols listed below along with their intended interpretations, where boldface denotes the formal symbol while lightface denotes the "real" (metamathematical) symbol:

(1) $\boldsymbol{S}$ (successor): $\boldsymbol{S}^{\mathfrak{N}} = S$, where $S(x) = x + 1$ for all $x \in \mathbb{N}$
(2) $\boldsymbol{+}$ (addition): $\boldsymbol{+}^{\mathfrak{N}} = +$
(3) $\boldsymbol{\times}$ (multiplication): $\boldsymbol{\times}^{\mathfrak{N}} = \times$

(4) $<$ (less than): $<^{\mathfrak{N}} = <$
(5) $\mathbf{0}$ (zero): $\mathbf{0}^{\mathfrak{N}} = 0$

The abbreviation $\widetilde{n}$ is pronounced *the numeral n*, and it stands for

$$\underbrace{S\ldots S}_{n \text{ of them}}\mathbf{0}$$

As they are metamathematical abbreviations, we are not using boldface type for numerals. □

**I.8.2 Definition.** A theory $\Gamma$ (this names the set of nonlogical axioms) over $L_{\mathfrak{N}}$ is *correct* over $\mathfrak{N}$ just in case $\mathscr{A} \in \Gamma$ implies $\models_{\mathfrak{N}} \mathscr{A}$.

That is, all its nonlogical axioms are true in $\mathfrak{N}$ (or really true, if $\mathfrak{N}$ happens to be the intended model). □

The term *correct* is used by Smullyan (1992). Some authors say "sound", but this is not as apt a terminology, for *sound* means something else: All first order theories are sound, but some theories over $L_{\mathfrak{N}}$ – although sound – may fail to be correct.

**I.8.3 Definition.** A theory $\mathfrak{T}$ over some language $L$ is *simply complete*, or just *complete*, iff, for all sentences $\mathscr{A}$ over $L$, we have at least one of $\vdash_{\mathfrak{T}} \mathscr{A}$ and $\vdash_{\mathfrak{T}} \neg\mathscr{A}$.

It is *simply incomplete*, or just *incomplete*, otherwise. An incomplete theory thus fails to decide at least one sentence $\mathscr{A}$ over $L$, that is, neither $\vdash_{\mathfrak{T}} \mathscr{A}$ nor $\vdash_{\mathfrak{T}} \neg\mathscr{A}$ holds.

Such an $\mathscr{A}$ is called an *undecidable sentence*. □

**Pause.** Why "sentence"? Why not define the above concepts (complete, etc.) in terms of arbitrary formulas over $L$?

Thus, in the case of an incomplete theory and for any particular one of its models – including the intended one – there is at least one sentence of the language which is (Tarski-)true in said model, but is not provable. Such is any undecidable sentence $\mathscr{A}$, for it or $\neg\mathscr{A}$ must be true in any given model.

An inconsistent theory is complete, of course.

**I.8.4 Definition.** A theory $\mathfrak{T}$ in the language of Peano arithmetic, $L_{\mathfrak{N}}$, is *ω-consistent* just in case there is no formula $\mathscr{A}(x)$ over $L_{\mathfrak{N}}$ such that all of the following hold:

$$\vdash_{\mathfrak{T}} \neg\mathscr{A}(\widetilde{n}) \qquad \text{for all } n \in \mathbb{N}$$

and $\vdash_{\mathfrak{T}} (\exists x)\mathscr{A}(x)$. Otherwise it is $\omega$-inconsistent. □

An $\omega$-consistent theory fails to prove something over its language; thus it is consistent. The converse is not true, a fact first observed by Tarski. This observation is a corollary of the techniques applied to prove Gödel's (first) incompleteness theorem (see our companion volume for the full story).

We can now state:

**I.8.5 Theorem (First Incompleteness Theorem, Semantic Version).** *Any correct extension of formal Peano arithmetic, effected in such a manner that the new set of axioms remains recognizable, will fail to prove at least one really true sentence.*

*It follows that any such extension is a simply incomplete theory.*

By "a set $A$ is *recognizable*" we mean that we can solve the membership problem, "$x \in A$?", by algorithmic, or mechanical, means. That is, in our case here, we can test any formula and find out, in a finite number of steps, whether it is an axiom or not. The technical term is *recursive*, but we do not intend to get into that here.[†]

The first word in the theorem is very important: "any". It shows that the theory (Peano arithmetic) is not just *incomplete* (take the trivial extension that adds nothing) but, indeed, *incompletable*: For, add to Peano arithmetic one really true sentence that it fails to prove. This effects an extension that is correct (why?) and constitutes a recognizable set of axioms. Repeat now, adding a really true sentence that *this* theory cannot prove. And so on.

In particular, this says that each of these extensions misses not one but infinitely many really true sentences (after all, we are effecting an infinite sequence of extensions; after each extension there are infinitely many more to go).

Why is Gödel's theorem true? The idea (in Gödel's original proof) is very old, based on games ancient Greek philosophers liked to play: The so-called

[†] A fair amount of *recursion theory* is covered in volume 1, *Mathematical Logic*, where, in particular, recursive sets are defined and studied.

"liar's paradox".[†] Through an ingenious *arithmetization* of the language Gödel managed to construct a sentence $\mathscr{G}$ whose natural interpretation said "I am not a theorem".

Let us see then if Peano arithmetic (or a correct and recognizable extension[‡]) can prove $\mathscr{G}$. Well, if it can, then – by correctness *and* soundness[§] – $\mathscr{G}$ is really true, i.e., it is *not* a theorem. This contradicts what we have just assumed.

So it must be that $\mathscr{G}$ is *not* a theorem.

But then, $\mathscr{G}$ is really true, for it says just that. We found a true sentence, $\mathscr{G}$, that is not provable.

We have more. Since the theory is correct (and sound), and $\neg\mathscr{G}$ is really false, this latter sentence is not provable. Thus the theory (as extended) is simply incomplete; $\mathscr{G}$ is undecidable.

Where have we used, in the above argument, the part of the assumptions that requires the set of nonlogical axioms to be recognizable? We actually did not use it explicitly, since our argument was too far removed from the level of detail that would exhibit such dependences on assumptions.

Suffice it to say that, among other things, the assumption on recognizability prevents us from cheating – thus invalidating Gödel's theorem: Why don't we just add *all the really true* sentences to the set of axioms and form a *complete* extension of Peano arithmetic? Because the recognizability assumption does not allow this. Such an extension results to a *non*-recognizable set of axioms (cf. volume 1).

There is another way to look at the intuitive reason behind the incompletableness phenomenon. This relies on results of recursion theory. Imagine beings who live in a world where set theorists call a set *countable* just in a case a mechanical procedure, or algorithm, exists to enumerate all the set's members, possibly with repetitions. Such beings call any set that fails to be enumerable in this manner *uncountable*. Intuitively, in the eyes of the inhabitants of this world, this latter type of set has far too many objects.

In this world the set of theorems of any extension of Peano arithmetic, by an arbitrary recognizable set of new axioms, is countable. The reason can be seen intuitively as a consequence of the recognizability of the set of nonlogical

[†] Attributed to Epimenides. He, a Cretan, said: "All Cretans are liars". So, was his statement true? Gödel's proof is based on a variation of this. A person says: "I am lying." Well, is he, or is he not?

[‡] The exact form of $\mathscr{G}$ depends on the extension at hand.

[§] Soundness we have for free. Correctness guarantees the real truth of the nonlogical axioms. Soundness extends this to all theorems.

axioms. This property allows us to build systematically (algorithmically) an infinite list[†] of all theorems.

**Digression.** Here is how. To simplify matters assume that the alphabet of the language $L_{\mathfrak{N}}$ is finite (for example, variables are really the strings

$$v\underbrace{|\ldots|}_{n+1}v$$

denoting what we may call $v_n$, for $n \geq 0$, built from just two symbols, "$v$" and "|").

We convert every proof into a single string by adding a new symbol to our alphabet, say #, which is used as a separator and "glue" – between formulas – as we concatenate all the formulas of a proof into a single string, from left to right. We will still call the result of this concatenation a "proof".

We now form two separate infinite lists, algorithmically. The first is the list of *all strings* over the alphabet of $L_{\mathfrak{N}}$, as the latter was augmented by the addition of #. This listing can be effected by enumerating by string length, and then, within each length group, *lexicographically* (alphabetically).[‡]

The second list is built as follows. Every time a string $A$ is put in the first list, we test *algorithmically* whether or not $A$ is a proof. We can do this, for, firstly, we can recognize if it is of the *right form*, that is,

$$A_1\#A_2\#\ldots\#A_n$$

where each $A_i$ is a nonempty string over $L_{\mathfrak{N}}$.

Secondly, if it is of the right form, we can then check whether indeed $A$ is a proof: Whether or not $A_j$ is the result of a primary rule of inference applied to $A_i$ (and possibly to $A_k$) for some $i < j$ (and $k < j$) can be determined from the *form* of the strings $A_j$, $A_i$, and $A_k$. The same is true of whether $A_j \in \Lambda$ or not. Finally the *recognizability* assumption means that we can also check whether or not $A_j$ is nonlogical.

If (and only if) $A$ passes the above test, i.e., it is a proof, then we add its *last formula* (the one to the right of the rightmost #) to the second list.

Now, it turns out that in such a world the set of all really true sentences of arithmetic is uncountable (this is proved in volume 1). Thus, there are infinitely many really true sentences that are not provable, no matter which theory (that

[†] One can "build an infinite list algorithmically" is jargon that means the following: One has an algorithm which, for any $n \in \mathbb{N}$, will generate the $n$th element of the list in a finite number of steps.

[‡] We assume that we have fixed an alphabetical order of the finitely many symbols of our alphabet.

produces a countable set of theorems) we have constructed on top of Peano arithmetic.[†]

While Gödel worked with the $\mathscr{G}$ that says "I am not a theorem", his result was purely syntactic. We state it without proof below.

**I.8.6 Theorem (First Incompleteness Theorem, Syntactic Version).** *Any $\omega$-consistent extension of formal Peano arithmetic, effected in such a manner that the new set of axioms remains recognizable, has undecidable sentences, and thus is a simply incomplete theory. In particular, one can construct a formula $\mathscr{G}$ which says "I am not a theorem of this theory". This formula is undecidable.*

**I.8.7 Remark.** In Gödel's proof simple (ordinary) consistency suffices to prove the unprovability of $\mathscr{G}$. $\omega$-consistency is called upon to prove that $\neg\mathscr{G}$ is not a theorem either. □

With a *different* "$\mathscr{G}$" (let us call it $\mathscr{G}'$), Rosser extended I.8.6 to the following result:

**I.8.8 Theorem (Gödel-Rosser Incompleteness Theorem).** *Any (simply) consistent extension of formal Peano arithmetic, effected in such a manner that the new set of axioms remains recognizable, has undecidable sentences and thus is a simply incomplete theory.*

We already mentioned that $\omega$-consistency is strictly stronger than consistency. Similarly, it can be seen, once the details of the Gödel argument are laid out, that correctness is strictly stronger than $\omega$-consistency (cf. volume 1).

The second incompleteness theorem of Gödel is, more or less, a formalization of the first. In plain English, it says that one of the really true sentences that Peano arithmetic – or, for that matter, any consistent and recognizable extension – cannot prove is *its own consistency*.

[†] It is straightforward to see that if there were only finitely many really true sentences that the formal system missed, these could be put into a finite table $T$, which we can check for membership, trivially. But then, we have an algorithm that can check a formula for membership in the set union between the theory's axioms and $T$ (just search the table; if not found there, then search the set of nonlogical axioms). Thus, adding the formulas of $T$ to the theory, we have an extension with a recognizable set of axioms. This new theory trivially has all the formulas in $T$ as theorems. Hence it has all the really true formulas as theorems ($T$ is all that the original theory missed), contradicting the fact that this set is uncountable, while the set of theorems is still countable.

This fact showed that Hilbert's finitary techniques, in the metatheory, were inadequate for his purposes: Intuitively, finitary techniques are codable by integers and therefore can be expressible and usable in formal Peano arithmetic.

Now we have two conflicting situations: Hilbert's belief that finitary techniques can settle the consistency (or otherwise) of formal theories has had as a corollary the expectation that Peano arithmetic could settle (prove) its own consistency (via the formalized finitary tools used *within* the theory). On the other hand, Gödel's second incompleteness theorem proved that this cannot be done.

**I.8.9 Theorem (Gödel's Second Incompleteness Theorem).** *Any (simply) consistent extension of formal Peano arithmetic, effected in such a manner that the new set of axioms remains recognizable, is unable to prove its own consistency.*

The detailed proof takes several tens of pages to be fully spelled out (cf. volume 1). However, the proof idea is very simple: Let us fix attention on an extension $\mathscr{T}$ as above, and let "Con" be a sentence whose natural interpretation (over $\mathfrak{N}$) says that $\mathscr{T}$ is consistent. Let also $\mathscr{G}$ be the sentence that says "I am not a theorem of $\mathscr{T}$".

Now, Gödel's first theorem (partly) asserts the truth (over $\mathfrak{N}$) of

$$\text{Con} \to \mathscr{G} \tag{1}$$

i.e., "if $\mathscr{T}$ is consistent, then $\mathscr{G}$ is true – hence, is not provable, for it says just that".

The quoted sentence above is correct, for $\omega$-consistency came into play only to show that Gödel's $\mathscr{G}$ was not *refutable*. This part of the first theorem is not needed towards the proof of the second incompleteness theorem.

Imagine now that we have managed to formalize the argument leading to (1) so that instead of truth in $\mathfrak{N}$ we can speak of provability in $\mathscr{T}$:[†]

$$\vdash_{\mathscr{T}} \text{Con} \to \mathscr{G}$$

It follows that if $\vdash_{\mathscr{T}}$ Con, then $\vdash_{\mathscr{T}} \mathscr{G}$ by modus ponens, contradicting the first incompleteness theorem.

[†] While this is in principle possible – to formalize the argument that leads to the truth of (1) – this is not exactly how one proves the deducibility of (1), and hence the second incompleteness theorem, in practice.

**I.8.10 Remark.** The contribution of Peano arithmetic is that it allows one to carry out Gödel's arithmetization formally, and to speak about provability, within the formal theory. In particular, it allows *self-reference*.[†]

Clearly, this machinery exists in all consistent (and recognizable[‡]) extensions of Peano arithmetic. It also exists in formal theories that may not be, exactly, extensions but are powerful enough to "contain", or, more accurately, *simulate* Peano arithmetic. Such a theory is ZFC set theory. Clearly it is not an extension, for the languages do not even match. However we can see that since ZFC is the foundation of all mathematics, in particular one must be able to do arithmetic within ZFC.[§]

Thus the incompletableness phenomenon manifests itself in ZFC as well. In particular, ZFC has undecidable sentences (first incompleteness theorem), and it cannot prove its own consistency (second incompleteness theorem).[¶] □

## I.9. Exercises

**I.1.** Prove that the closure of $\mathscr{I} = \{3\}$ under the two relations $z = x + y$ and $z = x - y$ is the set $\{3k : k \in \mathbb{Z}\}$.

**I.2.** The pair that effects the definition of **Term** (I.1.5, p. 13) is unambiguous.

**I.3.** The pair that effects the definition of **Wff** (I.1.8, p. 15) is unambiguous.

**I.4.** With reference to I.2.13 (p. 26), prove that if all the $g_Q$ and $h$ are defined everywhere on their input sets (i.e., they are "total"), that is, $\mathscr{I}$ for $h$ and $A \times Y^r$ for $g_Q$ and $(r + 1)$-ary $Q$, then $f$ is defined everywhere on $\mathrm{Cl}(\mathscr{I}, \mathscr{R})$.

**I.5.** Prove that for every formula $\mathscr{A}$ in **Prop** (I.3.2, p. 29) the following is true: Every nonempty proper prefix (I.1.4, p. 13) of the string $A$ has an excess of left brackets.

[†] Briefly, imagine that through arithmetization we have managed to represent every formula, and every sequence of formulas, of $L_{\mathfrak{N}}$ by a *numeral*. Gödel defined a formula $\mathscr{P}(x, y)$ which "says" that the formula coded $x$ is provable by a proof coded $y$. Self-reference allows one to find a natural number $n$ such that the numeral $\widetilde{n}$ codes the formula $\neg(\exists y)\mathscr{P}(\widetilde{n}, y)$. Clearly, this last formula says that "the formula coded by $\widetilde{n}$ is not a theorem". But it is talking about itself, for $\widetilde{n}$ is its own code. In short, $\mathscr{G} \equiv \neg(\exists y)\mathscr{P}(\widetilde{n}, y)$.

[‡] Recognizability is at the heart of being able to "talk about" provability within the formal theory.

[§] More concretely, and without invoking faith, one can easily show that there is an interpretation, in the sense of Section I.7, of Peano arithmetic within ZFC. This becomes clear in Chapter V, where the set of formal natural numbers, $\omega$, is defined.

[¶] The formal statement of the incompleteness theorems starts with the hypothesis "If ZFC is consistent".

**I.6.** Prove that any non-prime $\mathscr{A}$ in **Prop** has uniquely determined immediate predecessors.

**I.7.** For any formula $\mathscr{A}$ and any two valuations $v$ and $v'$, $\bar{v}(\mathscr{A}) = \bar{v}'(\mathscr{A})$ if $v$ and $v'$ agree on all the propositional variables that occur in $\mathscr{A}$.

**I.8.** Prove that $\mathscr{A}[x \leftarrow t]$ is a formula (whenever it is defined) if $t$ is a term.

**I.9.** Prove that Definition I.3.12 does not depend on our choice of new variables $\vec{z}_r$.

**I.10.** Prove that $\vdash (\forall x)(\forall y)\mathscr{A} \leftrightarrow (\forall y)(\forall x)\mathscr{A}$.

**I.11.** Prove I.4.23.

**I.12.** Prove I.4.24.

**I.13.** (1) Show that $x < y \vdash y < x$ ($<$ is some binary predicate symbol; the choice of symbol here is meant to provoke).

(2) Show informally that $\nvdash x < y \to y < x$
(*Hint*. Use the soundness theorem.)

(3) Does this invalidate the deduction theorem? Explain.

**I.14.** Prove I.4.25.

**I.15.** Suppose that $\Gamma \vdash t_i = s_i$ for $i = 1, \ldots, m$, where the $t_i, s_i$ are arbitrary terms. Let $\mathscr{F}$ be a formula, and $\mathscr{F}'$ be obtained from it by replacing any number of occurrences of $t_i$ in $\mathscr{F}$ (*not necessarily all*) by $s_i$. Prove that $\Gamma \vdash \mathscr{F} \leftrightarrow \mathscr{F}'$.

**I.16.** Suppose that $\Gamma \vdash t_i = s_i$ for $i = 1, \ldots, m$, where the $t_i, s_i$ are arbitrary terms. Let $r$ be a term, and $r'$ be obtained from it by replacing any number of occurrences of $t_i$ in $r$ (*not necessarily all*) by $s_i$. Prove that $\Gamma \vdash r = r'$.

**I.17.** Settle the "Pause" following I.4.21.

**I.18.** Prove I.4.27.

**I.19.** Prove that $\vdash x = y \to y = x$.

**I.20.** Prove that $\vdash x = y \land y = z \to x = z$.

**I.21.** Prove (semantically, without using soundness) that $\mathscr{A} \models (\forall x)\mathscr{A}$.

**I.22.** Suppose that $x$ is not free in $\mathscr{A}$. Prove that $\vdash \mathscr{A} \to (\forall x)\mathscr{A}$ and $\vdash (\exists x)\mathscr{A} \to \mathscr{A}$.

**I.23.** Prove the distributive laws:

$$\vdash (\forall x)(\mathscr{A} \land \mathscr{B}) \leftrightarrow (\forall x)\mathscr{A} \land (\forall x)\mathscr{B} \quad \text{and}$$
$$\vdash (\exists x)(\mathscr{A} \lor \mathscr{B}) \leftrightarrow (\exists x)\mathscr{A} \lor (\exists x)\mathscr{B}.$$

**I.24.** Prove $\vdash (\exists x)(\forall y)\mathscr{A} \to (\forall y)(\exists x)\mathscr{A}$ with two methods: first using the auxiliary constant method, next exploiting monotonicity.

**I.25.** Prove $\vdash (\exists x)(\mathscr{A} \to (\forall x)\mathscr{A})$.

In what follows let us denote by $\Lambda_1$ the pure logic of Section I.3 (I.3.13 and I.3.15). Let us now introduce a new pure logic, which we will call $\Lambda_2$. This is exactly the same as $\Lambda_1$, except that we have a different axiom group **Ax1**. Instead of adopting *all* tautologies, we only adopt the following four logical axiom schemata of group **Ax1**:[†]

(1) $\mathscr{A} \vee \mathscr{A} \to \mathscr{A}$
(2) $\mathscr{A} \to \mathscr{A} \vee \mathscr{B}$
(3) $\mathscr{A} \vee \mathscr{B} \to \mathscr{B} \vee \mathscr{A}$
(4) $(\mathscr{A} \to \mathscr{B}) \to (\mathscr{C} \vee \mathscr{A} \to \mathscr{C} \vee \mathscr{B})$

$\Lambda_2$ is due to Hilbert (actually, he also included associativity in the axioms, but, as Gentzen has proved, this was deducible from the system as here given; therefore, it was not an independent axiom – see Exercise I.35). In the exercises below we write $\vdash_i$ for $\vdash_{\Lambda_i}$, $i = 1, 2$.

**I.26.** Show that for all $\mathscr{F}$ and set of formulas $\Gamma$, if $\Gamma \vdash_2 \mathscr{F}$ holds then so does $\Gamma \vdash_1 \mathscr{F}$.

Our aim is to see that the logics $\Lambda_1$ and $\Lambda_2$ are equivalent, i.e., have exactly the same theorems. In view of the trivial Exercise I.26 above, what remains to be shown is that every tautology is a theorem of $\Lambda_2$. One particular way to prove this is through the following sequence of $\Lambda_2$-facts.

**I.27.** Show the transitivity of → in $\Lambda_2$:

$$\mathscr{A} \to \mathscr{B}, \mathscr{B} \to \mathscr{C} \vdash_2 \mathscr{A} \to \mathscr{C} \qquad \text{for all } \mathscr{A}, \mathscr{B}, \text{ and } \mathscr{C}.$$

**I.28.** Show that $\vdash_2 \mathscr{A} \to \mathscr{A}$ (i.e., $\vdash_2 \neg\mathscr{A} \vee \mathscr{A}$) for any $\mathscr{A}$.

**I.29.** For all $\mathscr{A}, \mathscr{B}$ show that $\vdash_2 \mathscr{A} \to \mathscr{B} \vee \mathscr{A}$.

**I.30.** Show that for all $\mathscr{A}$ and $\mathscr{B}$, $\mathscr{A} \vdash_2 \mathscr{B} \to \mathscr{A}$.

**I.31.** Show that for all $\mathscr{A}$, $\vdash_2 \neg\neg\mathscr{A} \to \mathscr{A}$ and $\vdash_2 \mathscr{A} \to \neg\neg\mathscr{A}$.

**I.32.** For all $\mathscr{A}$ and $\mathscr{B}$, show that $\vdash_2 (\mathscr{A} \to \mathscr{B}) \to (\neg\mathscr{B} \to \neg\mathscr{A})$. Conclude that $\mathscr{A} \to \mathscr{B} \vdash_2 \neg\mathscr{B} \to \neg\mathscr{A}$.
(*Hint.* $\vdash_2 \mathscr{A} \to \neg\neg\mathscr{A}$.)

**I.33.** Show that $\mathscr{A} \to \mathscr{B} \vdash_2 (\mathscr{B} \to \mathscr{C}) \to (\mathscr{A} \to \mathscr{C})$ for all $\mathscr{A}, \mathscr{B}, \mathscr{C}$.

[†] ¬ and ∨ are the primary symbols; →, ∧, ↔ are defined in the usual manner.

**I.34.** (Proof by cases in $\Lambda_2$.) Show for all $\mathscr{A}, \mathscr{B}, \mathscr{C}, \mathscr{D}$,

$$\mathscr{A} \to \mathscr{B}, \mathscr{C} \to \mathscr{D} \vdash_2 \mathscr{A} \vee \mathscr{C} \to \mathscr{B} \vee \mathscr{D}$$

**I.35.** Show for all $\mathscr{A}, \mathscr{B}, \mathscr{C}$ that
(1) $\vdash_2 \mathscr{A} \vee (\mathscr{B} \vee \mathscr{C}) \to (\mathscr{A} \vee \mathscr{B}) \vee \mathscr{C}$ and
(2) $\vdash_2 (\mathscr{A} \vee \mathscr{B}) \vee \mathscr{C} \to \mathscr{A} \vee (\mathscr{B} \vee \mathscr{C})$.

**I.36.** *Deduction theorem in "propositional"* $\Lambda_2$. Prove that if $\Gamma, \mathscr{A} \vdash_2 \mathscr{B}$ *using only modus ponens*, then also $\Gamma \vdash_2 \mathscr{A} \to \mathscr{B}$ *using only modus ponens*, for any formulas $\mathscr{A}, \mathscr{B}$ and set of formulas $\Gamma$.
(*Hint.* Induction on the length of proof of $\mathscr{B}$ from $\Gamma \cup \{\mathscr{A}\}$, using the results above.)

**I.37.** *Proof by contradiction in "propositional"* $\Lambda_2$. Prove that if $\Gamma, \neg\mathscr{A}$ derives a contradiction in $\Lambda_2$ *using only modus ponens*,[†] then $\Gamma \vdash_2 \mathscr{A}$ *using only modus ponens*, for any formulas $\mathscr{A}$ and set of formulas $\Gamma$. Also prove the converse.

We can now prove the *completeness theorem* (Post's theorem) for the "propositional segment" of $\Lambda_2$, that is, the logic, $\Lambda_3$ – so-called *propositional logic* (or *propositional calculus*) – obtained from $\Lambda_2$ by keeping only the "propositional axioms" (1)–(4) and modus ponens, dropping the remaining axioms and the $\exists$-introduction rule.

**Note.** It is trivial that if $\Gamma \vdash_3 \mathscr{A}$, then $\Gamma \vdash_2 \mathscr{A}$.

Namely, we will prove that, for any $\mathscr{A}$ and $\Gamma$, if $\Gamma \models_{\mathbf{Taut}} \mathscr{A}$, then $\Gamma \vdash_3 \mathscr{A}$.
First, a definition:

**I.9.1 Definition (Complete Sets of Formulas).** A set $\Gamma$ is *complete* iff for every $\mathscr{A}$, at least one of $\mathscr{A}$ or $\neg\mathscr{A}$ is a member of $\Gamma$. □

**I.38.** Let $\Gamma \nvdash_3 \mathscr{A}$. Prove that there is a complete $\Delta \supseteq \Gamma$ such that also $\Delta \nvdash_3 \mathscr{A}$. This is a *completion* of $\Gamma$.
(*Hint.* Let $\mathscr{F}_0, \mathscr{F}_1, \mathscr{F}_3, \ldots$ be an enumeration of all formulas. There *is* such an enumeration, right?
Define $\Delta_n$ by induction on $n$:

$$\Delta_0 = \Gamma$$
$$\Delta_{n+1} = \begin{cases} \Delta_n \cup \{\mathscr{F}_n\} & \text{if } \Delta_n \cup \{\mathscr{F}_n\} \nvdash_3 \mathscr{A} \\ \Delta_n \cup \{\neg\mathscr{F}_n\} & \text{otherwise} \end{cases}$$

[†] That is, it proves some $\mathscr{B}$ but also proves $\neg\mathscr{B}$.

To make sense of the above definition, show the impossibility of having both $\Delta_n \cup \{\mathscr{F}_n\} \vdash_3 \mathscr{A}$ and $\Delta_n \cup \{\neg\mathscr{F}_n\} \vdash_3 \mathscr{A}$. Then show that $\Delta = \bigcup_{n\geq 0} \Delta_n$ is as needed.)

**I.39.** (Post.) If $\Gamma \models \mathscr{A}$, then $\Gamma \vdash_3 \mathscr{A}$.
(*Hint.* Prove the contrapositive. If $\Gamma \nvdash_3 \mathscr{A}$, let $\Delta$ be a completion (Exercise I.38) of $\Gamma$ such that $\Delta \nvdash_3 \mathscr{A}$. Now, for every *prime formula* (cf. I.3.1, p. 29) $\mathscr{P}$, exactly one of $\mathscr{P}$ or $\neg\mathscr{P}$ (why exactly one?) is in $\Delta$. Define a *valuation* (cf. I.3.4, p. 30) $v$ on all prime formulas by

$$v(\mathscr{P}) = \begin{cases} 0 & \text{if } \mathscr{P} \in \Delta \\ 1 & \text{otherwise} \end{cases}$$

Of course, "0" codes, intuitively, "**true**", while "1" codes "**false**".
To conclude, prove by induction on the formulas of **Prop** (cf. I.3.2, p. 29) that the extension of $v$, $\overline{v}$, satisfies, for all formulas $\mathscr{B}$, $\overline{v}(\mathscr{B}) = 0$ iff $\mathscr{B} \in \Delta$. Argue that $\mathscr{A} \notin \Delta$.)

**I.40.** If $\Gamma \models_{\mathbf{Taut}} \mathscr{A}$, then $\Gamma \vdash_2 \mathscr{A}$.

**I.41.** For any formula $\mathscr{F}$ and set of formulas $\Gamma$, $\Gamma \vdash_1 \mathscr{F}$ iff $\Gamma \vdash_2 \mathscr{F}$.

**I.42.** *Compactness of propositional logic.* We say that $\Gamma$ is *finitely satisfiable* (*in the propositional sense*) iff every finite subset of $\Gamma$ is satisfiable (cf. I.3.6, p. 31). Prove that $\Gamma$ is satisfiable iff it is finitely satisfiable.
(*Hint.* Only the if part is non-trivial. It uses Exercise I.39. Further hint: If $\Gamma$ is unsatisfiable, then $\Gamma \models_{\mathbf{Taut}} \mathscr{A} \wedge \neg\mathscr{A}$ for some formula $\mathscr{A}$.)

# II

# The Set-Theoretic Universe, Naïvely

This volume is an introduction to *formal (axiomatic) set theory*. Putting first things first, we are attempting in this chapter to gain an intuitive understanding of the "real" universe of sets and the process of set creation (that is, what we think is going on in the metatheory). After all, we must have some idea of what it is that we are called upon to codify and *formally* describe before we embark upon doing it.

Set theory, using as primitives the notions of *set* (as a synonym for "collection"), *atom* (i.e., an object that is not subdivisible, not a collection), and the relation *belongs to* ($\in$), has sufficient expressive power to serve as the foundation of all mathematics. Mathematicians use notation and results from set theory in their everyday practice. We call the sets that mathematicians use the "real sets" of our mathematical intuition.

The exposition style in this chapter, true to the attribute "naïve", will be rather leisurely to the extent that we will forget, on occasion, that our "Chapter 0" (Chapter I) is present.[†]

## II.1. The "Real Sets"

*Naïvely*, or informally, set theory is the study of collections of "mathematical objects".

**II.1.1 Informal Description (Mathematical Objects).** Set theory is only interested in *mathematical objects*. As far as set theory is concerned, such objects

[†] It is our experience that readers of books like this one often choose to ignore "Chapter 0" initially. Invariably they are compelled to acknowledge its existence sooner or later in the course of the exposition. This will probably happen as early as Chapter III in our case.

are either

(1) *atomic* – let us understand by this term an object that is not a collection of other objects – such as a number or a point on a Euclidean line, or
(2) *collections* of mathematical objects. □

The foregoing description of "mathematical object" is *inductive* – describing the notion in terms of itself[†] – and, as all inductive descriptions do, it implies a formation of such objects, from the bottom up, by stages (cf. I.2.9). That is, we start with atoms.[‡] We may then collect atoms to form all sorts of first level collections, or *sets* as we will normally say. We may proceed to collect any mix of atoms and first-level sets to build new collections – that is, second level sets – and so on. Much of what set theory does is to attempt to remove the fuzziness from the foregoing description, and it does so by logically developing the properties of these sets.

**II.1.2 Example.** Thus, at the beginning we have all the level-0, or type-0, objects available to us. For example, atoms such as 1, 2, 13, $\sqrt{2}$ are available. At the next level we can include any number of such atoms (from none at all in one extreme, to all available atoms in the other extreme) to build a set, that is, a new mathematical object. Allowing the usual notation, i.e., listing within braces what we intend to include, we may cite a few examples of level-1 sets:

**L1-1.** $\{\}$. Nothing listed. This set has the standard notation $\emptyset$, and is known as the "*empty set*".
**L1-2.** $\{1\}$.
**L1-3.** $\{1, 1\}$.
**L1-4.** $\{1, \sqrt{2}\}$.
**L1-5.** $\{\sqrt{2}, 1\}$.

**Pause.** Are the sets that we have displayed under **L1-2** and **L1-3** the same? (I mean, equal?) Same question for the sets under **L1-4** and **L1-5**. Our "understanding" is – gentle way of saying "we postulate" – that set equality is

[†] Taking for granted an understanding of the terms "atom" and "collection" as intuitively self-explanatory, we use them to *describe* the objects that set theory studies. We are purposely leaving out a description of what "mathematical" is supposed to mean. Suffice it to say that experience provides numerous examples of mathematical objects, such as numbers of all sorts, points, lines, vectors, matrices, groups, etc. Of course, one needs an experiential understanding of *atomic* mathematical objects only, since all the others are built from those as described in II.1.1.

[‡] Atoms are very often called "urelements", pronounced "ūr-élements" – an anglicized form of the German word *Urelemente* – "primeval elements".

"forgetful of structure" such as repetition or permutation of elements. This understanding will soon be formally codified by choosing an appropriate axiom for set equality.

We already can identify a few level-2 objects, using what (we already know) *is* available.

Note how the level of nesting of { }-brackets matches the level of the objects.

**L2-1.** $\{\emptyset\}$.
**L2-2.** $\{1, \{1\}\}$.
**L2-3.** $\{\{\sqrt{2}, 1\}\}$. □

**II.1.3 Informal Definition.** A *set* is a non-atomic mathematical object, as the latter is described in II.1.1 (p. 99). □

The above is not a mathematical definition, because it is not precise. It is only an understanding on which we will subsequently base our choice of axioms. We do not need to attempt to search for the "real, definitive ontology" of sets (whatever that may mean) in order to do set theory, any more than we bother to search for the real ontology of "number" or "point" before we allow ourselves to do number theory or geometry, respectively.

From the mathematical point of view we are content to have tools (axioms and rules of logic) that tell us how sets *behave* rather than what sets *are* – entirely analogously with our attitude towards points and lines when we do axiomatic geometry, or towards numbers when we do axiomatic arithmetic (see, for example, our development of Peano arithmetic in volume 1 of these lectures).

Nevertheless, we will accept throughout this volume the previous (inductive) intuitive description of sets (II.1.3), doing so not because of some deep philosophical conviction, but in the sense that we will let this *accepted*[†] ontology guide us to choose reasonable axioms.

[†] It cannot be emphasized strongly enough that "accepted" is a very important verb here. Different descriptions/ontologies of sets may be possible – for example, one that denies Principle 1 below. Compare with the similar situation in geometry. It is possible to imagine different types of geometry – Euclidean on one hand, and various non-Euclidean ones on the other – but one is free to say "I will *accept* Euclidean geometry as the 'true' depiction of the universe and then proceed to learn its theorems". All that the latter acceptance means is a *decision* to study a particular type of geometry.

For this process to be effective we have to understand some of the fine points of II.1.3. Thus we begin by "unwinding" the induction into an *iteration*. We obtain the following two *principles of set formation* that are taken as "obvious truths":[†]

**Principle 0.** We can form, or build, sets by stages as follows: At stage 0 we acknowledge the presence of atoms. At each subsequent stage we may form a mathematical object – a *set* – by collecting together (mathematical) objects provided these are available to us from previous stages.

☡ Principle 0 is worded so that it leaves open the possibility that there are some sets that are obtained outside this formation process. However, our accepted inductive definition of sets (II.1.3) requires the following as well: ☡

**Principle 1.** Every set is built at some stage.

☡☡ **II.1.4 Remark.** Principle 1 is too strong. Omitting it does not affect the applicability of set theory to mathematics, i.e., the status of the former as the "foundation" of the latter. Of course, we cannot omit this principle unless we modify the descriptions II.1.1 and II.1.3 (for reasons analogous to the phenomenon described in I.2.9).

Now, if Principle 1 holds, as it does under our assumptions, then it leads to the *foundation axiom*. This comment will make much more sense later. For now, if you have just read it you have done so at your own risk. □ ☡☡

The following subsidiary (and delightfully vague) principle is important enough to be listed:

**(Subsidiary) Principle 2.** If our intuition will accept the existence of a stage (let us call it $\Sigma$) that *follows* all the (earliest) stages of construction (as a *set*) of *each* non-atomic member of some collection $A$, then $A$ *is* a mathematical object, and hence is a set ($A$ is not atomic, being a collection). The reason: By invoking Principle 0 we can built $A$ at stage $\Sigma$.

[†] Not less "obvious" than II.1.3, from which they follow directly. The reader may peek once more into I.2.9 for motivation, forewarned though that the stages of set formation are "far too many" to be numbered solely by natural numbers.

By the way, we do not normally speak of formation of atoms. Atoms are given outright. It is *sets* that we build.

**II.1.5 Remark.** (1) We are not saying above that stage $\Sigma$ is the "earliest" stage at which $A$ can be built, since we have said "follows" rather than "immediately follows".

(2) If some set is definable ("buildable") at some stage $\Sigma$, then we find it both convenient and intuitively acceptable to agree that it is also definable at any later stage as well. This corresponds to the common experience that a theorem has proofs of various lengths; once a "short" proof has been given, then – for example by adding redundant axioms in this proof – we can lengthen it arbitrarily and yet still have it yield the same theorem.

(3) "If our intuition will accept . . . ". This condition in Principle 2 creates some difficulty. *Whose* intuition? What is acceptable to some might not be to others.

This is a problem that arises when one does one's mathematics like a Platonist. A Platonist accepts some "obvious truths" about mathematical objects, and then proceeds to discover some more truths by employing (informal) logical deductions. Most practising mathematicians practise their craft like Platonists (whether they are card-carrying Platonists or not).

The catch with this approach, especially when applied to something "big" – by this I mean "foundational" – like set theory, is that one cannot always synchronize the understandings of all Platonists as to what *are* the "obvious truths" (about sets) – from where all reasoning begins to flow. There was a time not too long ago, for example, that mathematicians, otherwise comfortable with infinite sets, were not unanimous on whether the set-theoretic principle known as the axiom of choice was valid or not.

In the end, we avoid this difficulty by adopting the axiomatic approach to set theory. The Platonist within each of us may continue thinking of the sets that were imperfectly described in II.1.3 as the "real sets" – the ones that, Platonistically speaking, "exist". However, we plan to learn about sets by arguing like *formalists*. That is, we will translate *a few obvious and important truths* about real sets into a formal language (these translations will lead to our axiom schemata) and then employ first order logic as our reasoning tool to learn about real sets, *indirectly*, by proving theorems in our formal language.†

Thus, once the imprecise set-formation-by-stages thesis has motivated the selection of the above-mentioned "few obvious and important truths", it will

† The indirection occurs because in this language we will use terms to represent or codify real sets, and formulas to represent or codify *properties* of real sets. The reader who has read volume 1 is by now familiar with this approach, which we applied there in Chapter II to the study of (Peano) arithmetic. For terminology – such as "formal language", "term", "formula", "metatheory" – and tools from logic, the reader is referred to Chapter I of the present volume.

never be invoked again. Indeed, the opposite will happen. Our axioms will be strong enough to precisely define (eventually) what stages *are* and what happens at each stage, something that we are totally powerless to do now. □

Another criticism of the Platonist's approach to set theory is that it may entail contradictions (often called *antinomies* or *paradoxes*) which are hard to work around. Such paradoxes come about in the Platonist approach because it is not always clear what is a safe "truth" that we can adopt as a starting point of our reasoning. For example, is the following a "safe truth"? "For any *property* '$\mathscr{A}$' we can build a *set* of all the objects $x$ that satisfy $\mathscr{A}$." We look into this question in the next section. We also ponder briefly, through an example immediately below, the nature of set-building, or set-*defining*, "properties".

*A bit on terminology here*: Some people call the contradictions of *naïve* set theory "antinomies" (e.g., the Russell antinomy), and the harmless pleasantries of the Berry type "paradoxes". Others, like ourselves, use just one term, *paradoxes*. The reader may wish to decide for himself on the choice of terminology here, given that both words are rooted in Greek and a *paradox* is something that is "against one's belief" or even "against one's knowledge" ($\delta o\kappa\acute{\tilde{\omega}}$ = "I believe", or, "I know") while *antinomy* means being "against the – here, logical or mathematical – law" ($\nu\acute{o}\mu o\varsigma$ = "(the) law").

By the way, Berry's paradox is this: Define $n$ by "$n$ is a positive integer definable using fewer than 1000 non-blank symbols of print".[†] Examples of possible values of $n$: "5", "10", "10 raised to the power 350000", "the smallest prime number that has at least 10 raised to the power 350000 digits".

Now, the set of such numbers is finite, since there are finitely many ways to write a definition employing fewer than 1000 non-blank symbols. Thus, there are plenty of positive integers that are *not* so definable. Let $m$ denote the *smallest* such.

Then "$m$ is the smallest positive integer *not* definable using fewer than 1000 non-blank symbols of print".

Hey, we have just *defined* $m$ in less than 1000 non-blank symbols of print. A contradiction![‡]

**II.1.6 Remark.** It should be pointed out that our Platonist's view of "real sets" is informed by the work of Russell (and the later work of von Neumann),

[†] There is an implicit understanding that the set of *all available* symbols of print is finite: e.g., nowadays we could take as such the set of symbols on a standard English computer keyboard.

[‡] Well, not really. Neither of the statements "$n$ is a positive integer definable using fewer than 1000 non-blank symbols of print" or "$m$ is the smallest positive integer *not* definable using fewer than 1000 non-blank symbols of print" is a *definition*. What does "definable" mean?

namely, by his suggested "fix" for the paradox that he discovered – see next section. Georg Cantor, the founder of set theory, did not require any particular manner, or order, in which sets are formed. The axioms of the ZFC set theory of Zermelo and Fraenkel describe the von Neumann universe, which is built *by stages*, rather than the Cantorian universe. In the latter, as many sets can be present at once as our thought or perception will allow.[†] □

## II.2. A Naïve Look at Russell's Paradox

Let us ponder an elementary but fundamental example of what sort of contradictions might occur in the informal approach.

**II.2.1 Example.**[‡] Let us recall (from Chapter I or from our previous mathematics courses) that the notation

$$S = \{x : \mathscr{A}[x]\} \tag{1}$$

denotes (naïvely) the set $S$ of all objects $x$ that satisfy the formula $\mathcal{A}[x]$.[§] This means that entrance into $S$ is determined by

$$x \in S \quad \text{iff} \quad A[x] \tag{2}$$

where, of course, by "$x \in S$" we mean "$x$ is a member of $S$".

Let us see why the "Russell set"

$$R = \{x : x \notin x\} \tag{3}$$

is bad news for the informal approach: By (2), (3) yields

$$x \in R \quad \text{iff} \quad x \notin x \tag{4}$$

Now, since the variable $x$ can receive as value any object of the theory, in particular it can receive the "set" $R$. Thus, (4) yields the contradiction

$$R \in R \quad \text{iff} \quad R \notin R \tag{5}$$

Our only way out of the contradiction (5) is to say that

$R$ is not a set.[¶]

[†] In Cantor's own description, a set is any collection into "a whole" of objects of our "perception or of our thought".

[‡] Reminder: This is at the informal level.

[§] The square and round bracket notation is introduced in I.1.11.

[¶] This saves the theory, for now, since then it is "illegal" to plug $R$ into the set/atom variable $x$; hence (5) will *not* be derived from (4).

Here is what happened: We have obtained *outrageously many* $x$'s, each satisfying $x \notin x$. We then decided to collect them all, and build a set $R$. Our blunder was that we did not verify that Principle 2 (p. 102) applied to $R$.

No checking, no right to claim sethood for $R$!

Thus, the fact that $R$ is not a set is neither a surprise nor paradoxical. Apparently we have run out of stages. By the time all the $x$'s were built, there was no next stage left at which we could collect them all into a set $R$.

You are shaking your head. But consider this: $x \in x$ has to be *false* for any object $x$. Indeed, it is trivially false for atomic $x$. For non-atomic $x$, in order to build the copy to the right of "$\in$" I must first have (at an earlier stage[†]) the $x$ to the left of "$\in$" (since it is a member of the collection $x$).

Thus $x \notin x$ is true for all objects $x$. But then $R$ contains *everything*, for the entrance condition in (3) is always true. No wonder there were no stages left to build $R$. We have used them all up building the $x$'s! □

Now that we realize that some collections such as $S$ in (1) above are sets, and some are not, how can we tell which is which? The axiomatic approach resolves such issues in an elegant way.

## II.3. The Language of Axiomatic Set Theory

Having taken our foregoing terse description of how sets are built – by stages – as our (Platonist) view of what sets really are, we now want to avoid embarrassing paradoxes and to turn the theory into a consistent deductive science. The obvious approach is to translate or codify naïve set theory into a formal *first order theory*, in the sense of Chapter I. We begin by choosing a formal first order language, $L_{\text{Set}}$.

$L_{\text{Set}}$ has the standard *logical symbols*, namely,

$$\exists,\ \neg,\ \vee,\ =,\ (,\ )$$

[†] "Hmm", the alert reader will say. "You are using Principle 1 here. You are saying that if $x$ is a non-atomic mathematical object, then it *must* be built at some stage." Indeed! However, even if we were to totally abandon Principle 1 and revise our naïve picture of the universe of "mathematical objects" to allow $x \in x$ to be true (depending on the "value" of $x$), we could still avoid the Russell paradox argument in exactly the same way we avoid it in the presence of Principle 1: Namely, by *restricting* the circumstances where the "operation" $\{x : A[x]\}$ is allowed to build a set. In short, it is not the choice of an answer to the question "$x \in x$" that creates the Russell paradox, rather it is a *comprehension principle*, $\{x : A[x]\}$, that is far too powerful for its own good.

and object variables, that is, variables that *when interpreted* are interpreted to take as values (real) sets or atoms,[†]

$$v_0, v_1, \ldots, v_i, \ldots$$

Additionally, $L_{\text{Set}}$ has the two *primitive nonlogical* symbols "$\in$"[‡] and "$U$".[§] The former is a binary predicate that is intended to mean (when interpreted) "is a member of". The latter is a unary predicate meant to say (of its argument) "is an atom". All the remaining familiar symbols of set theory (e.g., $\cap$, $\cup$, $\subseteq$, $\times$) are introduced as *defined nonlogical* symbols as the theory progresses.

Of course, exactly as in Chapter I, one introduces, in the interest of convenience, *defined logical symbols*, namely, $\forall$, $\wedge$, $\rightarrow$, $\leftrightarrow$.

The logical axioms and rules of first order logic will be those that we have introduced in Chapter I.

Our *intended* "standard model" – i.e., *what we are describing by our formal system* – is the already (imperfectly) described "universe" of all sets and atoms.[¶] Having here a standard model in mind, which the axiomatic theory attempts to describe correctly and completely,[#] is entirely analogous to what we did in volume 1.

There we had the standard model of arithmetic, $\mathfrak{N} = (\mathbb{N}, S, +, \times, 0, <)$, in mind, and each of the axiomatizations introduced, **ROB** and **PA**, were successive attempts at formally deducing all the true formulas of $\mathfrak{N}$ from a few axioms.[||]

[†] This is the implementation of our intentions regarding the nature of "mathematical objects" (II.1.1).

[‡] "$\in$" is a stylized form of $\varepsilon$ (épsilon) the first letter of the ancient Greek word "εστί" (pronounced *estí* – with a short " i " – and meaning "is"). Thus, if $y$ is the set of all even integers, $x \in y$ says that "$x$ *is* an even integer". Some authors still use $x \,\varepsilon\, y$ instead of $x \in y$, but we prefer not to do so, as "$\varepsilon$" is overused (e.g., empty string, epsilon number, Hilbert selector, a major contributor to the dreaded "$\varepsilon$-$\delta$" proofs of calculus, etc.).

[§] "Primitive" means "primeval" or "given at the very beginning".

[¶] Known as the von Neumann universe. That this universe is not a set – it is equal to the Russell collection $R$ granting Principle 1, is it not? – is an issue we should not worry about, as long as we accept that its *members* are *all* the sets and atoms.

[#] The terms *correctness* and (syntactic or simple) *completeness* of a theory are defined in I.8.2 and I.8.3. The former means that every theorem is true when interpreted in the standard model. The latter means that all formulas that are true in the standard model are theorems. We have no difficulty with the former requirement. The latter is impossible by Gödel's incompleteness theorems (I.8.5).

[||] Again, we could not produce *all* such formulas, because of Gödel's incompleteness theorems.

The choice of the intended model influences the choice of (nonlogical) axioms. We will adopt in this book the Zermelo-Fraenkel axioms (ZF) *with* the axiom of choice as an additional axiom. This system is known as ZFC.

**II.3.1 Remark.** To an observer we will appear to behave like *formalists*, manipulating sets and their properties in a finitistic manner, writing proofs within a first order theory.

Sets will be[†] just terms of our language, thus finite symbol sequences! Properties of sets will also be finite objects, the formulas of the language. Finally, proofs themselves are finite objects, being finite sequences of formulas.

We do not have to take sides or disclose where our loyalties lie – Platonist vs. formalist camp – as such disclosure is functionally irrelevant. What really matters is how we *act* when we form deductions.[‡] □

The definitions of terms and formulas for $L_{\text{Set}}$ are those given in Chapter I (I.1.5 and I.1.8) subject to the restriction that the only primitive nonlogical symbols are the two predicates $\in$ and $U$.

**II.3.2 Remark (Basic Language).** Thus, the terms of $L_{\text{Set}}$ are just the variables, $v_0, v_1, v_2, \ldots$.

Formulas are built from the *atomic* ones, that is, $Uv_i$, $v_i = v_j$, and $v_i \in v_j$ for all choices of $i, j$ in $\mathbb{N}$, by application of the connectives $\neg$, $\vee$, and $\exists$ (I.1.8).

We call $L_{\text{Set}}$ the *basic* or *primitive* language of set theory. The qualifiers "basic" and "primitive" reflect the fact that the only nonlogical symbols are the primeval $\in$ and $U$. As the theory is being developed, we will frequently introduce new *defined* symbols, thus extending $L_{\text{Set}}$ (cf. Section I.6). This process also enlarges the variety of terms (adding terms such as $\emptyset$, $\{x : \neg x = x\}$, $\omega$, etc.) and formulas.

We note that the definitions of terms and formulas of $L_{\text{Set}}$ are strictly about syntax – i.e., correct *form*. Thus they do not concern themselves with semantic issues or provability issues. In particular, it is good form to write "$v_2 \in v_2$", even if one of our axioms will entail that "$v_2 \in v_2$" is a false statement.[§] □

[†] "Be" is used here in formalist jargon. The Platonist terminology is "be denoted by".

[‡] A true formalist would probably declare that the sets of our intuition do not really "exist" – mathematically speaking – and sets just ***are*** the terms of our formal language. See Bourbaki (1966b, p. 62), where it is stated, in translation, that "[ . . . ] the word 'set' will be strictly considered to be a synonym for 'term'; in particular, phrases such as 'let $x$ be a set' are, in principle, totally superfluous, since every variable *is* a term; such phrases are simply introduced to help the intuitive interpretation of [formal] texts".

[§] We have already remarked in II.2.1 that $x \in x$ is false in our intended universe.

**II.3.3 Remark (Notational Liberties).** In practice we use *abbreviations* – in the metalanguage – in order to enhance readability. The reader may wish to review the metalinguistic *argot* introduced in Chapter I, in particular the agreement that calligraphic upper case (Latin) letters stand for formulas (see Remark I.1.9 for more on this) while $t, s, r$ typically are metasymbols for arbitrary terms.

We also take liberties with the correct syntax of formulas and terms, writing them down in abbreviated more readable form.[†] One type of abbreviation has to do with reducing the number of brackets that we use when we write formulas. This has been discussed in Chapter I.

We also have metalinguistic abbreviations for the variables we use. Instead of the cumbersome $v_{1234777}$, $v_{90}$, etc., we adopt the convention that *any* lower or upper case *single* Latin letter, with or without subscripts or primes, will denote an object variable.

We will *prefer* to name variables using letters near the end of the alphabet. Nevertheless, we will often introduce variables such as $A$, $b$, $c$, or even go to Greek and German (*Fraktur*) alphabets to obtain names for variables, such as $\alpha$, $\beta$ and $\mathfrak{m}$, $\mathfrak{k}$.

We will almost never write down a well-formed formula of set theory (except for the purpose of mocking its unfriendliness and awkwardness). We will prefer "translations" of the formula in our *argot*, where abbreviations of various sorts, and natural language, *are* allowed. This renders the formula easier to read and comprehend. □

**II.3.4 Example.** Picking up the last comment above, we show here two examples of what the judicious use of English saves us from:

(a) We would sooner say "$n$ is a natural number" than write the set theory formula

$$\begin{aligned}&(\forall x)(\forall y)(x \in y \in n \to x \in n) \wedge \\ &\qquad [n = \emptyset \vee (\exists x)(\neg U(x) \wedge n = x \cup \{x\}] \wedge \\ (\forall m)\Big[m \in n \to \Big\{&(\forall x)(\forall y)(x \in y \in m \to x \in m) \wedge \\ &\qquad [m = \emptyset \vee (\exists x)(\neg U(x) \wedge m = x \cup \{x\}]\Big\}\Big]\end{aligned}$$

It should be noted that the above is already abbreviated. It contains the defined symbols $\emptyset$, $\cup$ and $\{x\}$, not to mention that the variables used were

[†] "Abbreviated" is not always shorter. $+x \times yz$ is shorter than $x + (y \times z)$, and $ft_1t_2t_3$ is shorter than $f(t_1, t_2, t_3)$. Yet the longer forms are easier to understand. An *abbreviation* here is an alternative, easier to understand form.

written in *argot* and that we employed logical abbreviations such as →, ∀, etc., and brackets of various shapes.

(b) If we are in number theory (arithmetic) we would sooner state "$n$ is a prime", than

$$n > S0 \wedge (\forall x)(\forall y)(n = x \times y \to x = S0 \vee x = n) \qquad \square$$

## II.4. On Names

The reader is referred to Section I.1 (in particular see the discussion starting with Remark I.1.3 on p. 10) so that we will not be unduly repetitive in the present section.

**II.4.1 Remark (The Last Word on "Truth").** The completeness theorem shows that the syntactic apparatus of a first order (formal) logic totally captures the semantic notion of truth, "modulo" the acceptance as true of any given assumptions, $\Gamma$. This justifies the habit of the mathematician (even of the formalist – see Bourbaki (1966b, p. 21)) of saying – in the context of any given theory $\Gamma$ – "it is true", meaning "it is a $\Gamma$-theorem", or "it is $\Gamma$-proved"; "it is false", meaning "the negation is a $\Gamma$-theorem"; "assume that $\mathscr{A}$ is true", meaning "add the formula $\mathscr{A}$ – to $\Gamma$ – as a nonlogical axiom"; and "assume that $\mathscr{A}$ is false", meaning "add to $\Gamma$ the formula $\neg\mathscr{A}$, as a nonlogical axiom".

There is another meaning (and use) of "true" which is *not* equivalent to deducibility. This is what we have called the "really true", meaning what is true in the *intended*, or *standard*, model.

The Gödel incompletableness phenomenon tells us that strong theories like set theory or arithmetic will never[†] have deducibility coincide with "real truth". This is because there will always be sentences $\mathscr{A}$ that are neither provable nor refutable – but one of them surely is "really true"!

We plan to abandon the qualifier "real" (as we promised in an earlier footnote) and the quotes around *true* (in the standard model). To avoid confusion with the "other" *true* ( $=$ deducible) we will do the following:

*Whenever we mean "is proved" or "is provable", we just say so. We will not say "is true" instead.* □

It will be convenient (and it is standard practice) to use the symbol sequences that are terms of the formal theory as *names* for their counterparts, real sets of the

[†] "Never" as long as all consistent augmentations of the set of axioms preserve the set's recursiveness – or "recognizability".

metatheory. For example, in the metatheory we may say "the set $\{x : \neg x = x\}$", thus using the symbol sequence "$\{x : \neg x = x\}$" to name some appropriate real set, the so-called *empty set*.[†]

This correspondence between certain terms[‡] of the type "$\{x : \mathscr{A}[x]\}$" and real sets is nothing else than an application of first order definability (cf. I.5.15). That is, if some real set $A$ is first order definable in the standard model by a formula $\mathscr{A}$, we have

$$x \in A \quad \text{iff} \quad \mathscr{A}(x) \text{ is true in the standard model}$$

Thus the *symbol sequence* $\mathscr{A}$, or more suggestively the symbol sequence $\{x : \mathscr{A}(x)\}$, can name the set $A$. As we know, the latter sequence is pronounced "the set of all $x$ such that $\mathscr{A}(x)$ is true".

Reciprocally, in our *argot*, we nickname *formal* terms and their formal abbreviations by the metamathematical (often English) names of the sets that they name. Thus, e.g., we say that $\{x : \neg x = x\}$, or $\emptyset$, *is* "the empty set of the (formal) theory".

We note two limitations of this naming apparatus below.

**II.4.2 Remark (Limitations of our Naming Mechanism).**

(a) *Inconvenience*. This stems from the fact that formal terms, even for very simple sets, can be horrendously long, and thus can be quite incomprehensible. For this reason we almost always introduce, via *formal definitions*, short names for such terms (formal abbreviations) that we just make up – that is, we name the formal names by more convenient (shorter) names that we invent. These shorter defined names become part of the *formal language* of the formal theory. For example, the term $\{x : \neg x = x\}$ is formally abbreviated by a new (defined) constant symbol, $\emptyset$.

(b) *Formal limitations*. First, we cannot name – that is, first order define – *all* the real sets by terms, because there are far more sets than terms that we can supply via the formal language. We cannot even so define all the subsets of the set of natural numbers. As a consequence, we cannot codify all "properties" of sets in our language as formulas either, because there are far too many properties but too few formulas.[§] Second, as if the short supply

[†] I am guilty here of borrowing from the sequel. "$\{x : \neg x = x\}$" is *not* a term of the basic language II.3.2; instead it is a *defined term*, about which we will talk soon.

[‡] Russell's paradox is fresh in our memory; thus, "certain" is an apt qualifier.

[§] We cannot gloss over this shortage of names by extending $L_{\text{Set}}$ by the addition of a name for each real set. That would make our language impractical, as it would make it uncountable, and of formulas were not limiting enough, Gödel's first incompleteness theorem yields another insurmountable limitation. It tells us that in *any* consistent axiomatization of set theory through a recognizable set of axioms there will be infinitely many "true properties" of sets *for each of which we do have a formal name*, but nevertheless none of these formal names (formulas of $L_{\text{Set}}$) are deducible in the formal theory. Thus the theory can only incompletely capture "real truth".

Unlike the limitation of convenience (a), which we have easily circumvented above, there is no solution for (b).

But then, why bother with a formal theory at all? I can state two reasons.

The first is the precision that such a theory gives to the *concept* of deduction, turning it into a mathematical (finite) object. Thus, questions such as "is our set theory free from contradiction?"[†] or "what is, and what is not, deducible from what axioms?" become meaningful and can be handled mathematically, *in principle*.

The above are metatheoretical concerns. The second reason has to do with everyday mathematical practice. We benefit from the precision that a formal theory gives to the *praxis* of deduction, guarding us against embarrassing paradoxes that loose arguments or loose assumptions may lead to. □

**II.4.3 Example.** *This, like most examples, is in the "real (informal) realm".* The natural numbers 0, 1, 2, ... when collected together form a set, normally denoted by $\mathbb{N}$.

We often capture the above sentence informally by writing $\mathbb{N} = \{0, 1, 2, \ldots\}$. □

**II.4.4 Remark.** $\mathbb{N}$ is a remarkable example of a (real) set, in that we have no easy way to give a term name for it in set theory. The next best thing to do is, instead, to find *another* real set, $\omega$, "isomorphic to $\mathbb{N}$",[‡] that can easily be seen to have a term counterpart in the formal theory.

Needless to say, as follows from our previous discussion, both the real $\omega$ and the corresponding formal term are denoted by the same symbol, $\omega$.

therefore impossible to *generate finitely*. In an uncountable language we will not be able to write, or even check, proofs anymore, as we will have trouble telling what symbols belong to $L_{\text{Set}}$ and which do not. As a result, we will be unable to know whether an arbitrary string of symbols is a formula, an axiom, or just rubbish.

[†] This is the original reason that prompted the development of axiomatic theories.

[‡] The reader should not worry about the meaning of "isomorphic". We will come back to this very issue in Chapter V.

Notwithstanding the comment regarding $\mathbb{N}$, we will continue employing it, as well as other familiar sets from the metatheory (such as $\mathbb{Z}$ (the integers), $\mathbb{Q}$ (the rationals), and $\mathbb{R}$ (the reals)) in our informal discussions, i.e., in examples, remarks, "naïve" exercises, etc. □

**II.4.5 Remark.** At the outset of Section II.3 we promised "to turn the theory into a *consistent* deductive science".

It may come as a shock to the reader that we have no (generally acceptable) proof of consistency of ZFC. We Platonistically got around the consistency question of either **ROB** or Peano arithmetic by saying "sure they are consistent; $\mathfrak{N}$ is a model of either", since few reasonable people will feel uncomfortable about $\mathfrak{N}$ or its fitness to certify consistency (serving as a model). Notwithstanding this, proof theorists have found alternative *constructive proofs* of the consistency of Peano arithmetic and hence of **ROB** (such proofs can be found in Schütte (1977) and Shoenfield (1967)). These proofs necessarily use tools that are beyond those included in Peano arithmetic (because of Gödel's second incompleteness theorem).

We have *no* such constructive proof of the consistency of ZFC. This, of course, is not surprising. Since ZFC satisfies Gödel's second incompleteness theorem, a proof of its consistency cannot be formalized within ZFC. Here then is the difficulty: What will any such consistency proof "outside" or "beyond" ZFC look like, considering that

(a) it cannot be expressed in ZFC, and yet
(b) ZFC, being the "foundation of all mathematics" (or such that "mathematics can be embedded" in it), ought to be able to include (formalizations of) all mathematical tools and mathematical reasoning – including a formalization of its consistency proof that was given "outside" ZFC.

However, most set theorists are willing to accept the consistency of ZFC. "Evidence" (but not a proof) of this consistency is, of course, the presence of the standard model. □

# III

# The Axioms of Set Theory

## III.1. Extensionality

Under what conditions are two sets equal?

First of all, if $a$ and $b$ stand for urelements, then $a = b$ just obeys the logical axioms of equality (Definition I.3.13, p. 35) and we have nothing to add about their behaviour concerning equality.

For sets, however, we *require* that they be equal whenever they contain exactly the same elements, regardless of whatever "structural connections" these elements may have. In order to state this axiom formally we use the primitive predicate of set theory, $U$. Thus $Ux$ is intended to mean "$x$ is an *urelement*" (therefore $\neg Ux$ will mean "$x$ is a *set*").

We use the "abbreviation"[†] "$U(x)$" for "$Ux$", since it is arguable that, in general, "$P(t_1, \ldots, t_n)$" is more user-friendly than "$Pt_1 \ldots t_n$".

**III.1.1 Axiom (Extensionality).**

$$\neg U(A) \wedge \neg U(B) \rightarrow \Big((\forall x)(x \in A \leftrightarrow x \in B) \rightarrow A = B\Big) \qquad (E)$$

*In words, for any* sets *A and B, if they have the same elements, then they are equal.*

**III.1.2 Remark.** We noted that the above axiom, $(E)$, indicates that we want two sets to be equal as long as they have the same elements, regardless of the existence of inner structure in the sets (such as one dimensional or higher

[†] We have already remarked in a footnote on p. 109 that an "abbreviation" is meant to create easier-to-read text, not necessarily shorter text.

dimensional order) and regardless of "intention", that is, *how* the set originally came about. For example, the set that contains the integers 2 and 3 is expected to be the same as (equal to) the set of all roots of $x^2 - 5x + 6 = 0$, despite the difference in the two descriptions. That is, *we have postulated that set equality is "forgetful of structure"*.

It is the *extension* of a set (i.e., its actual contents) that decides equality, hence the name of Axiom III.1.1.

But is this axiom "true"?[†] Is this the condition that governs equality of "real" sets? Well, formal or axiomatic mathematics aims at *representing* reality within an artificial but formal and precise language. In this "representation" there is always something lost, partly due to limitations of the formal language and partly due to *decisions* that we make – regarding the choice of our assumptions, or axioms – about what features of "reality" are *essential* (of which we create counterparts in the formal language) and which are not.

For example, a "real" line has width no matter how you construct it, but geometers have decided that width is irrelevant, so they invent their lines so as to have no width. In our case, we are saying that to decide set equality we forget all attributes of sets other than what elements they contain. This is what we deem to be important.

Now that we have defended our choice of $(E)$, another question arises: *Is* $(E)$ a *definition*? Much of the elementary literature on the theory of sets takes the point of view that it is (see Wilder (1963, p. 58), for example), although often somewhat casually.

A formal definition would introduce the symbol "=" by $(E)$, *if* the symbol were not part of our "logical list" of symbols. Since we already have "=" and its basic axioms, $(E)$, for us, is an axiom.[‡] □

Note that in the extensionality axiom we state no more than what we need – following the mathematician's known propensity to assume less in order to have the pleasure of proving more. This accounts for using "$\cdots \rightarrow A = B$" rather than "$\cdots \leftrightarrow A = B$". In fact, we have

$$\vdash \neg U(A) \wedge \neg U(B) \rightarrow \Big(A = B \rightarrow (\forall x)(x \in A \leftrightarrow x \in B)\Big) \qquad (1)$$

where "$\vdash$" indicates provability without using any nonlogical axioms.

[†] Remember that while we cannot give a *proof* of consistency of ZFC, we can at least check that its axioms are "really true", i.e., true in the standard model. This checking is done on the informal level, of course.

[‡] In fact, a formal definition is still an axiom, via which a new formal symbol is introduced – as we saw in Section I.6. But this is not the case with $(E)$.

To see this, note that

$$\vdash A = B \to (x \in A \leftrightarrow x \in B)$$

by equality axioms. Then, since $A = B$ has no free $x$,[†] ∀-introduction (cf. I.4.5, p. 44) yields

$$\vdash A = B \to (\forall x)(x \in A \leftrightarrow x \in B)$$

(1) now follows by tautological implication (cf. I.4.1, p. 43).

We have said that urelements have no set-theoretic structure, that is, if $b$ is an urelement, then the claim $a \in b$ is false for all possible meanings of $a$. This is formalized below.

**III.1.3 Axiom (Urelements are "Atomic").**

$$U(y) \to \neg(\exists x)x \in y$$

The above says that urelements do not have any elements; however, that does *not* make them empty sets, for urelements are not sets. The content of III.1.3 can also be written as

$$U(y) \to (\forall x)\neg x \in y$$

or even

$$U(y) \to (\forall x)x \notin y$$

where "$x \notin y$" is an *informal* (metamathematical) abbreviation of "$\neg x \in y$".

**III.1.4 Remark.** The contrapositive of III.1.3 is

$$(\exists x)x \in y \to \neg U(y)$$

that is, intuitively, "if $y$ has any elements, then it is a set".

It is also useful to note the consequence

$$x \in y \to \neg U(y)$$

of the above (substitution axiom $x \in y \to (\exists x)x \in y$ and tautological implication). □

**III.1.5 Definition (Subsets, Supersets).** We introduce to the formal language a new predicate of arity 2, denoted by "⊆", by the defining axiom

$$A \subseteq B \leftrightarrow (\forall x)(x \in A \to x \in B) \tag{1}$$

[†] $A$ and $B$ are free variables distinct from $x$.

In English, *in the case where $A$ and $B$ are sets*, this says – that is, the *semantics* in the *metatheory* is – that $A \subseteq B$ is a short name for the statement "every member of $A$ is also a member of $B$".

We read "$A \subseteq B$" as "$A$ is a *subset* of $B$", or "$B$ is a *superset* of $A$". Instead of $A \subseteq B$ we sometimes write $B \supseteq A$. As usual, we negate $\subseteq$ and $\supseteq$ by writing $\not\subseteq$ and $\not\supseteq$ respectively. □

**III.1.6 Remark.** In III.1.5 we chose to allow the symbol $\subseteq$ to act on *any objects* of set theory – sets or atoms. An alternative approach that is often adopted in the literature on naïve set theory is to make $A \subseteq B$ *undefined* (or meaningless) if either $A$ or $B$ is an atom (this would be analogous to the situation in Euclidean geometry, where, for example, parallelism is undefined on, say, triangles or circles). Our choice in III.1.5, that is, (1), is technically more convenient, since it does not require us to know the exact nature of $A$ or $B$ before we can use the (formal) abbreviation $A \subseteq B$.

We note that, according to III.1.5, $x \in A \rightarrow x \in B$ is provable if $A$ is an urelement (by III.1.3), that is, $A \subseteq B$ is provable. Indeed,

$$U(A) \vdash_{\mathrm{ZFC}} (\forall x)\neg x \in A$$

by Axiom III.1.3 and modus ponens. Thus,

$$U(A) \vdash_{\mathrm{ZFC}} \neg x \in A \tag{2}$$

by specialization (cf. I.4.6, p. 44). By tautological implication followed by generalization (I.4.8) we get what we want from (2):

$$U(A) \vdash_{\mathrm{ZFC}} (\forall x)(x \in A \rightarrow x \in B)$$

or, applying the deduction theorem (I.4.19),

$$\vdash_{\mathrm{ZFC}} U(A) \rightarrow (\forall x)(x \in A \rightarrow x \in B)$$

We use the provability symbol with a subscript, e.g., $\vdash_{\mathscr{T}}$, to indicate in which theory $\mathscr{T}$ (i.e., with what nonlogical axioms) we carry out the proof. In the simple proofs above we have used the subscript ZFC, but we only employed Axiom III.1.3. We will seldom indicate what subset of ZFC axioms we are using at any given moment, and whenever we do, we will normally do so in words rather than using some $\vdash$-subscript different from ZFC.

The reader will also note that "$\mathscr{A} \vdash_{\mathscr{T}} \ldots$" is the same as "$\mathscr{T} + \mathscr{A} \vdash \ldots$" or "$\mathscr{T} \cup \{\mathscr{A}\} \vdash \ldots$" □

**III.1.7 Example.** Since $x \in a \to x \in a$ is a tautology (note the absence of subscript on the $\vdash$ that follows), we have $\vdash x \in a \to x \in a$ and hence

$$\vdash (\forall x)(x \in a \to x \in a) \tag{$*$}$$

by generalization. Thus, by III.1.5 and tautological implication,

$$\vdash a \subseteq a \tag{$**$}$$

or *any object is a subset of itself.*

We did not use a subscript (e.g., ZFC) on $\vdash$ immediately above because no ZFC axioms were used. □

We immediately infer from III.1.1 and III.1.5 the following Proposition III.1.8.

**III.1.8 Proposition.** *For any two* sets *$A$ and $B$,*

$$A = B \leftrightarrow A \subseteq B \wedge B \subseteq A$$

*holds, or, formally,*

$$\vdash_{\text{ZFC}} \neg U(A) \wedge \neg U(B) \to (A = B \leftrightarrow A \subseteq B \wedge B \subseteq A)$$

An observation is in order in connection with the above: Logical connectives have lower priority than any other connectives, so that "$A \subseteq B \wedge B \subseteq A$" means "$(A \subseteq B) \wedge (B \subseteq A)$".

*Proof.* Invoking the deduction theorem (I.4.19), we prove instead

$$\neg U(A), \neg U(B) \vdash_{\text{ZFC}} A = B \leftrightarrow A \subseteq B \wedge B \subseteq A \tag{1}$$

We offer a calculational proof:

$$
\begin{aligned}
& A \subseteq B \wedge B \subseteq A \\
\leftrightarrow\ & \Big\langle \text{III.1.5 and the equivalence theorem (I.4.25, p. 52)} \Big\rangle \\
& (\forall x)(x \in A \to x \in B) \wedge (\forall x)(x \in B \to x \in A) \\
\leftrightarrow\ & \Big\langle \forall \text{ over } \wedge \text{ distributivity (Exercise I.23, p. 95)} \Big\rangle \\
& (\forall x)\Big((x \in A \to x \in B) \wedge (x \in B \to x \in A)\Big) \\
\leftrightarrow\ & \Big\langle \text{tautological equivalence and equivalence theorem} \Big\rangle \\
& (\forall x)(x \in A \leftrightarrow x \in B) \\
\leftrightarrow\ & \Big\langle \text{extensionality, } \textit{plus assumptions} \text{ for “}\to\text{”; Leibniz axiom for “}\leftarrow\text{”} \Big\rangle \\
& A = B
\end{aligned}
$$

□

It often happens that $A \subseteq B$, yet $A \neq B$, where "$A \neq B$" is (informal) short for "$\neg A = B$".

**III.1.9 Definition (Proper Subsets).** We introduce a new predicate symbol of arity 2, denoted by "$\subset$", by the defining axiom

$$A \subset B \leftrightarrow A \subseteq B \wedge \neg A = B$$

We read "$A \subset B$" as "$A$ is a *proper* subset of $B$". □

The reader will note that, stylistically, $\subseteq$ and $\subset$ parallel the symbols $\leq$ and $<$ (compare how $a < b$, for numbers, means $a \leq b$ and $a \neq b$). It should be mentioned however that it is not uncommon in the literature (e.g., in Bourbaki (1966b), Shoenfield (1967)) to use $\subset$ where we use $\subseteq$, and then to need to use $\subsetneq$ or even $\subsetneqq$ to denote proper subset.

## III.2. Set Terms; Comprehension; Separation

We now want to imitate the informal act of collecting into a set all objects $x$ that satisfy (i.e., make true – in the standard model) a formula $\mathscr{A}[x]$. We already saw that a careless approach here entails dangers (Section II.2). We revisit this issue again here, and then provide a formal fix.

It is clear that the reasonable thing to do *within the formal theory* is to restrict attention to formulas $\mathscr{A}$ for which we can *prove* the existence of a set, say $a$, such that

$$x \in a \leftrightarrow \mathscr{A}[x]$$

is provable, thus replacing truth (cf. I.5.15 and also p. 111) by provability. We achieve this if we can prove

$$\vdash_{\mathrm{ZFC}} (\exists y)\Big(\neg U(y) \wedge (\forall x)(x \in y \leftrightarrow \mathscr{A}[x])\Big) \tag{1}$$

where we have taken the precaution that $y$ is not free in $\mathscr{A}$.[†] Bourbaki (1966b) calls formulas such as $\mathscr{A}$ "collecting".

As in *loc. cit.,* we use the symbol

$$Coll_x\mathscr{A} \tag{2}$$

[†] Otherwise we would be attempting to "solve" for $y$ in something like "$x \in y \leftrightarrow \mathscr{A}(x, y)$", which is *not* the same as collecting in a container called $y$ all those "values" of $x$ that make $\mathscr{A}(x, z)$ "true" for *an arbitrarily chosen* value of the "parameter" $z$. Such rather obvious remarks will become sparser as we go along.

as an abbreviation of

$$(\exists y)\Big(\neg U(y) \wedge (\forall x)(x \in y \leftrightarrow \mathscr{A}[x])\Big)$$

Note that $x$ is not a free variable in (1) (or in (2)), but it is, nevertheless, *the free variable of interest* in $\mathscr{A}$, the variable whose "values" (that "satisfy" $\mathscr{A}$) we are determined to collect. (2) says that indeed we *can* collect these "values" into a set.

**III.2.1 Example.** We verify that *if* $y$ *is a set, then* $Coll_x x \in y$. It will be best to give a terse annotated proof of the formal translation of the italicized statement, that is,

$$\vdash_{\text{ZFC}} \neg U(y) \to Coll_x x \in y \tag{$A$}$$

It is easier to tackle instead

$$\neg U(y) \vdash_{\text{ZFC}} (\exists z)\Big(\neg U(z) \wedge (\forall x)(x \in z \leftrightarrow x \in y)\Big) \tag{$B$}$$

where $z$ is distinct from $y$ and $x$:

(1) $\neg U(y)$ $\Big\langle$given$\Big\rangle$

(2) $x \in y \leftrightarrow x \in y$ $\Big\langle$tautology, hence logical axiom$\Big\rangle$

(3) $(\forall x)(x \in y \leftrightarrow x \in y)$ $\Big\langle$(2) plus *generalization* (I.4.8, p. 45)$\Big\rangle$

(4) $\neg U(y) \wedge (\forall x)(x \in y \leftrightarrow x \in y)$ $\Big\langle$(1), (3) plus taut. implication$\Big\rangle$

(5) $\neg U(y) \wedge (\forall x)(x \in y \leftrightarrow x \in y) \to$
$(\exists z)\Big(\neg U(z) \wedge (\forall x)(x \in z \leftrightarrow x \in y)\Big)$ $\Big\langle$logical axiom$\Big\rangle$

(6) $(\exists z)\Big(\neg U(z) \wedge (\forall x)(x \in z \leftrightarrow x \in y)\Big)$ $\Big\langle$(4), (5), and modus ponens$\Big\rangle$

We also note that, by the deduction theorem, $(B)$ yields

$$\vdash_{\text{ZFC}} \neg U(y) \to (\exists z)\Big(\neg U(z) \wedge (\forall x)(x \in z \leftrightarrow x \in y)\Big) \tag{$C$}$$

which is an expanded notation for $(A)$. Intuitively, all of $(A)$, $(B)$, and $(C)$ say that if $y$ is a set, then ZFC allows us to collect all the $x$ for which $x \in y$ is true *into a set*. This is hardly surprising at the intuitive level, since this collection that we form is just $y$ – and we already know it is a set. Nevertheless, it is reassuring that we have had no bad surprises here. □

**III.2.2 Example (Russell's Paradox, Second Visit).** In this example we go out of our way to show that Russell's paradox can be argued within pure logic – in II.2.1 we *appeared* to be arguing within (informal) set theory – and that it has nothing to do with one's position on the set-theoretic question "$x \in x$?"

We prove that if $\mathscr{A}(x, y)$ and $\mathscr{B}(y)$ are *any* formulas,[†] then

$$\vdash \neg(\exists y)\Big(\mathscr{B}(y) \land (\forall x)(\mathscr{A}(x, y) \leftrightarrow \neg\mathscr{A}(x, x))\Big) \tag{$i$}$$

We prove ($i$) by contradiction (I.4.21, p. 51) combined with proof by auxiliary constant (I.4.27, p. 53):

$$(1)\ (\exists y)\Big(\mathscr{B}(y) \land (\forall x)(\mathscr{A}(x, y) \leftrightarrow \neg\mathscr{A}(x, x))\Big) \quad \Big\langle \text{added or "given"} \Big\rangle$$

$$(2)\ \mathscr{B}(c) \land (\forall x)(\mathscr{A}(x, c) \leftrightarrow \neg\mathscr{A}(x, x)) \quad \Big\langle \text{added; } c \text{ is a new constant} \Big\rangle$$

$$(3)\ (\forall x)(\mathscr{A}(x, c) \leftrightarrow \neg\mathscr{A}(x, x)) \quad \Big\langle (2) \text{ plus tautological implication} \Big\rangle$$

$$(4)\ \mathscr{A}(c, c) \leftrightarrow \neg\mathscr{A}(c, c) \quad \Big\langle (3) \text{ plus specialization} \Big\rangle$$

The formula in line (4) is, or creates, a contradiction, since also $\vdash \mathscr{A}(c, c) \leftrightarrow \mathscr{A}(c, c)$.

Taking $\mathscr{B}(y)$ to be the special case of $\neg U(y)$, and $\mathscr{A}(x, y)$ to be $x \in y$, we have refuted $Coll_x x \notin x$, that is, we have established that (note absence of subscript on $\vdash$) $\vdash \neg Coll_x x \notin x$ *without ever using any nonlogical axioms* or being aware of the question $x \in x$. Our third (and last) visit to Russell's paradox will show that what is at work here is a Cantor diagonalization.

Thus, Frege's (1893) *axiom of comprehension* that

for all formulas $\mathscr{A}$, one has $Coll_x \mathscr{A}$

is refutable within pure logic by providing the counterexample $\mathscr{A} \equiv x \notin x$.[‡] □

[†] You may want to look at I.1.11, p. 19.

[‡] The reader may recall that we have reserved "≡" for string equality, *not* formula equivalence (see p. 13).

Russell's paradox was not the first paradox discovered in naïve set theory as originally developed by Georg Cantor. The Burali-Forti antinomy had been suggested earlier, and we will get to it at the proper place in our development. Russell's paradox is less technical on the one hand, and is immediately relevant to our present discussion on the other hand; thus we opted for its early presentation.

Obviously, comprehension, as stated by Frege, was too strong and allowed some "super-collections" to be built (like $R$) which are *not* sets.

It should be noted here that in the work of Cantor the comprehension schema was used carefully so as not to construct "too large" or "too complicated" sets, as compared with the "ingredient" sets that entered into such constructions. For this reason, his work did not explicitly lead to Russell's objection, the latter being aimed at Frege.

We still want to be able to collect into a set all "$x$-values" that satisfy "reasonable" formulas $\mathscr{A}$ – leaving the unreasonable ones out. Let us work towards identifying such reasonable formulas. But first a lemma:

**III.2.3 Lemma.**

$$\vdash_{ZFC} \neg U(y) \wedge (\forall x)(x \in y \leftrightarrow \mathscr{A}) \wedge \neg U(z) \wedge (\forall x)(x \in z \leftrightarrow \mathscr{A}) \rightarrow y = z$$

*Proof.*

$$\begin{aligned}
& \neg U(y) \wedge (\forall x)(x \in y \leftrightarrow \mathscr{A}) \wedge \neg U(z) \wedge (\forall x)(x \in z \leftrightarrow \mathscr{A}) \\
\leftrightarrow\ & \Big\langle \forall \text{ over } \wedge \text{ distributivity, taut. equivalence and I.4.25, p. 52} \Big\rangle \\
& \neg U(y) \wedge \neg U(z) \wedge (\forall x)\Big((x \in y \leftrightarrow \mathscr{A}) \wedge (x \in z \leftrightarrow \mathscr{A})\Big) \\
\rightarrow\ & \Big\langle \forall\text{-monotonicity (I.4.24, p. 52) and taut. implication} \Big\rangle \\
& \neg U(y) \wedge \neg U(z) \wedge (\forall x)(x \in y \leftrightarrow x \in z) \\
\rightarrow\ & \Big\langle \text{extensionality – only this step used a ZFC axiom} \Big\rangle \\
& y = z
\end{aligned}$$

(Recall the discussion in I.7.11) □

**III.2.4 Remark.** Let us recall the basics of introducing new function symbols (Section I.6). Suppose that we have the following:

$$\vdash_{\mathscr{T}} (\exists y)\mathscr{A}(y, \vec{x}_n) \tag{1}$$

and

$$\vdash_{\mathscr{T}} \mathscr{A}(y, \vec{x}_n) \wedge \mathscr{A}(z, \vec{x}_n) \to y = z \tag{2}$$

Then we may introduce a new function symbol, say $f_{\mathscr{A}}$, *into the language of* $\mathscr{T}$ by the axiom

$$f_{\mathscr{A}}(\vec{x}_n) = y \leftrightarrow \mathscr{A}(y, \vec{x}_n) \tag{3}$$

We also know that (3) is provably equivalent to (4) below (see p. 73), so that (4) could serve as well as the introducing axiom:

$$\mathscr{A}(f_{\mathscr{A}}(\vec{x}_n), \vec{x}_n) \tag{4}$$

We finally recall (p. 73) the notation (Whitehead and Russell (1912)) for the term $f_{\mathscr{A}}(\vec{x}_n)$:

$$(\iota y)\mathscr{A}(y, \vec{x}_n) \tag{5}$$

A special case of the above is important. Suppose that $t(\vec{x}_n)$ is a term, where we have written "$(\vec{x}_n)$" to indicate the totality of free variables in $t$. Then substitution in the logical axiom $x = x$ yields $t = t$; thus the substitution axiom and modus ponens yield

$$\vdash (\exists y) y = t \tag{6}$$

Note the absence of subscript from $\vdash$ above. Since equality is transitive, we also have

$$\vdash y = t \wedge z = t \to y = z \tag{7}$$

We may thus introduce a new function symbol $f_t$ of arity $m \geq n$ by the axiom (form (3) above)

$$f_t(\vec{y}_m) = y \leftrightarrow t = y \tag{8}$$

or equivalently (form (4) above)

$$f_t(\vec{y}_m) = t \tag{9}$$

where the list $\vec{y}_m$ contains all the variables $\vec{x}_n$ of $t$.

An important, more general case of (1)–(2) often occurs in practice. We may have a proof of (1) for some, but not all, $\vec{x}_n$:

$$\vdash_{\mathscr{T}} \mathscr{D}(\vec{x}_n) \to (\exists y)\mathscr{A}(y, \vec{x}_n) \tag{10}$$

We assume that we still have (2) in the restricted form

$$\vdash_{\mathscr{T}} \mathscr{D}(\vec{x}_n) \rightarrow \mathscr{A}(y, \vec{x}_n) \wedge \mathscr{A}(z, \vec{x}_n) \rightarrow y = z \tag{11}$$

We would like now to introduce a function $f_{\mathscr{A}}$ that satisfies (3) (or (4)) for precisely those $\vec{x}_n$ that satisfy $\mathscr{D}$. We could define $f$ arbitrarily for those $\vec{x}_n$ for which $\mathscr{D}$ fails.

Let then $a$ be some constant in the language of $\mathscr{T}$. Let

$$\mathscr{B}(y, \vec{x}_n) \equiv \mathscr{D}(\vec{x}_n) \wedge \mathscr{A}(y, \vec{x}_n) \vee \neg\mathscr{D}(\vec{x}_n) \wedge y = a \tag{12}$$

We show that

$$\vdash_{\mathscr{T}} \mathscr{B}(y, \vec{x}_n) \wedge \mathscr{B}(z, \vec{x}_n) \rightarrow y = z \tag{13}$$

We will employ the deduction theorem:

$(i)$ $\mathscr{D}(\vec{x}_n) \wedge \mathscr{A}(y, \vec{x}_n) \vee \neg\mathscr{D}(\vec{x}_n) \wedge y = a$ $\langle$assume$\rangle$

$(ii)$ $\mathscr{D}(\vec{x}_n) \wedge \mathscr{A}(z, \vec{x}_n) \vee \neg\mathscr{D}(\vec{x}_n) \wedge z = a$ $\langle$assume$\rangle$

$(iii)$ $\mathscr{D}(\vec{x}_n) \wedge \mathscr{A}(y, \vec{x}_n) \wedge \mathscr{A}(z, \vec{x}_n) \vee \neg\mathscr{D}(\vec{x}_n) \wedge y = a \wedge z = a$

$\langle(i)$, $(ii)$ plus $\models_{\textbf{taut}}\rangle$

$(iv)$ $y = z$

$\langle$proof by cases: 1st disjunct of $(iii)$ plus (11); 2nd disjunct plus trans. of "="$\rangle$

We next note that

$$\vdash_{\mathscr{T}} (\exists y)\mathscr{B}(y, \vec{x}_n) \tag{14}$$

Indeed,

$(i)$ $\mathscr{D}(\vec{x}_n)$ $\langle$assume$\rangle$

$(ii)$ $(\exists y)\mathscr{A}(y, \vec{x}_n)$ $\langle(i)$, (10) and MP$\rangle$

$(iii)$ $\mathscr{A}(c, \vec{x}_n)$ $\langle$assume; $c$ is a new constant$\rangle$

$(iv)$ $\mathscr{D}(\vec{x}_n) \wedge \mathscr{A}(c, \vec{x}_n) \vee \neg\mathscr{D}(\vec{x}_n) \wedge c = a$ $\langle(i)$, $(iii)$ plus $\models_{\textbf{Taut}}\rangle$

$(v)$ $(\exists y)\big(\mathscr{D}(\vec{x}_n) \wedge \mathscr{A}(y, \vec{}x_n) \vee \neg\, \mathscr{D}(\vec{x}_n) \wedge y = a\big)$ $\langle(iv)$, subst. axiom plus MP$\rangle$

By the deduction theorem

$$\vdash_{\mathscr{T}} \mathscr{D}(\vec{x}_n) \rightarrow (\exists y)\mathscr{B}(y, \vec{x}_n) \tag{15}$$

Next consider

$$\begin{array}{lll}
(i) & \neg\mathscr{D}(\vec{x}_n) & \langle \text{assume} \rangle \\
(ii) & \neg\mathscr{D}(\vec{x}_n) \wedge a = a & \langle (i), \vdash a = a \text{ and } \models_{\mathbf{Taut}} \rangle \\
(iii) & \mathscr{D}(\vec{x}_n) \wedge \mathscr{A}(a, \vec{x}_n) \vee \neg\mathscr{D}(\vec{x}_n) \wedge a = a & \langle (ii) \text{ plus } \models_{\mathbf{Taut}} \rangle \\
(iv) & (\exists y)\big(\mathscr{D}(\vec{x}_n) \wedge \mathscr{A}(y, \vec{x}_n) \vee \neg\mathscr{D}(\vec{x}_n) \wedge y = a\big) & \langle (iii), \text{ subst. axiom} \\
 & & \quad \text{plus MP} \rangle
\end{array}$$

Thus, by the deduction theorem,

$$\vdash_{\mathscr{T}} \neg\mathscr{D}(\vec{x}_n) \to (\exists y)\mathscr{B}(y, \vec{x}_n) \tag{16}$$

(15) and (16) yield (14) via proof by cases. (13) and (14) allow the introduction of $f_{\mathscr{A}}$ by the axiom

$$\mathscr{B}(f_{\mathscr{A}}(\vec{x}_n), \vec{x}_n) \tag{17}$$

That is,

$$\mathscr{D}(\vec{x}_n) \wedge \mathscr{A}(f_{\mathscr{A}}(\vec{x}_n), \vec{x}_n) \vee \neg\mathscr{D}(\vec{x}_n) \wedge f_{\mathscr{A}}(\vec{x}_n) = a \tag{18}$$

Since

$$\mathscr{D}(\vec{x}_n), (18) \models_{\mathbf{Taut}} \mathscr{A}(f_{\mathscr{A}}(\vec{x}_n), \vec{x}_n)$$

and

$$\neg\mathscr{D}(\vec{x}_n), (18) \models_{\mathbf{Taut}} f_{\mathscr{A}}(\vec{x}_n) = a$$

we get

$$(18) \vdash_{\mathscr{T}} \mathscr{D}(\vec{x}_n) \to \mathscr{A}(f_{\mathscr{A}}(\vec{x}_n), \vec{x}_n) \tag{19}$$

and

$$(18) \vdash_{\mathscr{T}} \neg\mathscr{D}(\vec{x}_n) \to f_{\mathscr{A}}(\vec{x}_n) = a \tag{20}$$

In other words, (10) and (11) allow us to introduce a new function symbol $f_{\mathscr{A}}$ that satisfies (19) and (20). (20) defines $f_{\mathscr{A}}$ "arbitrarily" for those $\vec{x}_n$ where $\mathscr{D}$ fails.

It is easy to check, just as we did on p. 73, that (19) is provably equivalent to

$$(18) \vdash_{\mathscr{T}} \mathscr{D}(\vec{x}_n) \to \Big(\mathscr{A}(y, \vec{x}_n) \leftrightarrow y = f_{\mathscr{A}}(\vec{x}_n)\Big) \tag{19'}$$

$\square$ ☡

**III.2.5 Definition (Set Terms).** If $\vdash_{\mathrm{ZFC}}$ $Coll_x \mathscr{F}(x, \vec{z}_n)$, then Lemma III.2.3 allows us to introduce the term

$$(\iota y)\Big(\neg U(y) \wedge (\forall x)\big(x \in y \leftrightarrow \mathscr{F}(x, \vec{z}_n)\big)\Big) \tag{$st$}$$

We call the above a *set term, defined by the formula* $\mathscr{F}$ *and the objects* $z_1, \ldots, z_n$.

We (almost always) use the shorter, and standard, metamathematical abbreviation

$$\{x : \mathscr{F}(x, \vec{z}_n)\} \tag{$sst$}$$

instead of the notation $(st)$. □

The reader will recall from Section I.6 that, in actual fact, a formal definition introduces a *function symbol*, not a term. However, we agree to leave the "ontology" of that function symbol, say, "$f_{\mathscr{F}}$", unspecified, and we agree to use the *argot* $(st)$ or $(sst)$ above to informally denote the *term*, $f_{\mathscr{F}}(\vec{z}_n)$, that corresponds to $f_{\mathscr{F}}$.

Nevertheless, whenever $\vdash_{\mathrm{ZFC}}$ $Coll_x \mathscr{F}$, either of the notations $(st)$ or $(sst)$ *stands for (i.e., names) a formal term* of the theory.

It is important to note that *set terms* give rise to more complicated *terms* than just variables. The latter are the only terms of the basic language $L_{\mathrm{Set}}$ (see II.3.2), while as we enrich the language by the (formal) addition of new function symbols $f_{\mathscr{A}}$, $f_{\mathscr{B}}$, etc., and constants $\emptyset$, $\omega$, etc., we can build complicated terms such as $f_{\mathscr{A}}(\ldots, f_{\mathscr{B}}(\ldots, \omega, \ldots), \emptyset, \ldots)$ (see I.1.5). Such terms we will call just *terms* (or "formal terms", to occasionally emphasize their formal status).

We immediately have

**III.2.6 Proposition (Set Term Facts).** *If* $\vdash_{\mathrm{ZFC}}$ $Coll_x \mathscr{F}$, *then:*

*(i)* $\vdash_{\mathrm{ZFC}} y = \{x : \mathscr{F}\} \leftrightarrow \neg U(y) \wedge (\forall x)(x \in y \leftrightarrow \mathscr{F})$.
*(ii)* $\vdash_{\mathrm{ZFC}} \neg U\Big(\{x : \mathscr{F}\}\Big)$.
*(iii)* $\vdash_{\mathrm{ZFC}} x \in \{x : \mathscr{F}\} \leftrightarrow \mathscr{F}$.
*(iv) If also* $\vdash_{\mathrm{ZFC}}$ $Coll_x \mathscr{G}$, *then* $\vdash_{\mathrm{ZFC}} (\forall x)(\mathscr{F} \to \mathscr{G}) \leftrightarrow \{x : \mathscr{F}\} \subseteq \{x : \mathscr{G}\}$.
*(v) If also* $\vdash_{\mathrm{ZFC}}$ $Coll_x \mathscr{G}$, *then* $\vdash_{\mathrm{ZFC}} (\forall x)(\mathscr{F} \leftrightarrow \mathscr{G}) \leftrightarrow \{x : \mathscr{F}\} = \{x : \mathscr{G}\}$.

*Proof.* $(i)$: This is (3) in III.2.4 above, that is, the introductory axiom for "$f_{\mathscr{A}}$", where $\mathscr{A}$ is "$\neg U(y) \wedge (\forall x)(x \in y \leftrightarrow \mathscr{F})$".

$(ii)$: By (4) in III.2.4 and tautological implication.

$(iii)$: By (4) in III.2.4 and tautological implication followed by specialization.

$(iv)$: By $(iii)$ and the equivalence theorem,

$$\vdash_{\text{ZFC}} (\forall x)(\mathscr{F} \to \mathscr{G}) \leftrightarrow (\forall x)(x \in \{x : \mathscr{F}\} \to x \in \{x : \mathscr{G}\})$$

Note that the assumption $\vdash_{\text{ZFC}} Coll_x \mathscr{G}$ allows us to introduce $\{x : \mathscr{G}\}$ formally and have $(iii)$ (with $\mathscr{F}$ replaced by $\mathscr{G}$).

$(v)$: Similar to $(iv)$. □

In Section III.4 we will introduce informal notation that allows us to write $(i)$–$(v)$ above *in the metatheory* without requiring prior proofs of either $Coll_x \mathscr{F}$ or $Coll_x \mathscr{G}$.

**III.2.7 Remark.** Note that $x$ is a bound variable in $(st)$ of Definition III.2.5, and hence also in $(sst)$. Thus, if the conditions for the variant theorem are fulfilled (I.4.13, p. 46) – that $w$ occurs neither free nor bound in $\mathscr{F}$ – then we can also write the set term as $\{w : \mathscr{F}(w, \vec{z}_n)\}$. That is,

$$\vdash_{\text{ZFC}} \{x : \mathscr{F}(x, \vec{z}_n)\} = \{w : \mathscr{F}(w, \vec{z}_n)\} \tag{1}$$

The above is different from $(v)$ of III.2.6. It can be proved as follows:

$$\begin{aligned}
& y = \{x : \mathscr{F}(x, \vec{z}_n)\} \\
\leftrightarrow & \left\langle (i) \text{ of III.2.6} \right\rangle \\
& \neg U(y) \wedge (\forall x)(x \in y \leftrightarrow \mathscr{F}(x, \vec{z}_n)) \\
\leftrightarrow & \left\langle \text{variant theorem (I.4.13, p. 46) and equivalence theorem} \right\rangle \\
& \neg U(y) \wedge (\forall w)(w \in y \leftrightarrow \mathscr{F}(w, \vec{z}_n)) \\
\leftrightarrow & \left\langle (i) \text{ of III.2.6} \right\rangle \\
& y = \{w : \mathscr{F}(w, \vec{z}_n)\}
\end{aligned}$$

Thus,

$$\vdash_{\text{ZFC}} y = \{x : \mathscr{F}(x, \vec{z}_n)\} \leftrightarrow y = \{w : \mathscr{F}(w, \vec{z}_n)\}$$

from which, substitution and the logical fact $\vdash t = t$ for any term $t$ yield (1).

As a corollary we have – via the equivalence theorem and (1) – the well-known and obvious (under the usual non-occurrence restrictions on $w$)

$$\vdash_{\text{ZFC}} w \in \{x : \mathscr{F}[x]\} \leftrightarrow \mathscr{F}[w] \tag{2}$$

□

Formally introduced set terms play a dual role. On one hand, formally, they are just meaningless symbol sequences of which we have proved (or a proof exists, in any case) that they *are* sets. For that reason, we often just say "…the *set* $\{x : \mathscr{F}\}$…".

On the other hand, the formula part of a set term first order defines (in the standard structure) some real set; hence the term itself represents or names that set.

The very format of the chosen symbol for set terms,

$$\{x : \mathscr{F}\}$$

is suggestive of its semantics in the standard model: "the collection of all the $x$ that make $\mathscr{F}$ true". As a matter of fact, this is more than notational suggestiveness: Soundness of all first order theories – and anticipating that our axioms will be true in the standard model – implies that all ZFC theorems will be "really true". In particular, the formula in $(iii)$ of III.2.6 is "true" and says that "$x$ is in $\{x : \mathscr{F}[x]\}$ iff $\mathscr{F}[x]$ is 'true' for this $x$".

**III.2.8 Example.** We continue here what we have started in Example III.2.1. Since

$$\vdash_{\mathrm{ZFC}} \neg U(y) \to Coll_x x \in y$$

III.2.6 $(iii)$ gives

$$\neg U(y) \vdash_{\mathrm{ZFC}} x \in \{x : x \in y\} \leftrightarrow x \in y$$

By III.2.6 $(ii)$,

$$\neg U(y) \vdash_{\mathrm{ZFC}} \neg U\Big(\{x : x \in y\}\Big)$$

as well; hence

$$\neg U(y) \vdash_{\mathrm{ZFC}} y = \{x : x \in y\} \tag{1}$$

by extensionality via substitution.

In words, *every set is equal to a set term.* □

We now introduce a weak form of Frege comprehension, so that we can have a sufficient condition for $Coll_x \mathscr{A}$ to hold.

**III.2.9 Axiom (Schema: Separation or "Subsets" Axioms).** *For every formula $\mathscr{P}[x]$ which does not have any free occurrences of $y$, the following* *is an axiom:*

$$\neg U(A) \to (\exists y)\big(\neg U(y) \wedge (\forall x)(x \in y \leftrightarrow x \in A \wedge \mathscr{P}[x])\big)$$

*For short,*

$$\neg U(A) \to Coll_x\big(x \in A \wedge \mathscr{P}[x]\big)$$

The above is a *schema* due to the presence of the arbitrary formula $\mathscr{P}$. Every specific choice of $\mathscr{P}$ leads to an axiom: An *instance* of the axiom schema. The name "separation axiom" is apt since the axiom allows us to separate members from non-members (of a set).

Why is the schema III.2.9 true (in the standard model)? Well, it says that if $A$ is a set, then – no matter what formula $\mathscr{P}$ we choose – we can also collect

$$\text{all those } x \text{ that make } x \in A \wedge \mathscr{P}[x] \text{ true} \tag{1}$$

into a set.

Now, all those $x$ in (1) *are* in $A$, and we know that we have formed $A$ at some stage[†] (it is a set!), say $\Sigma$, that comes *after* all the stages at which *all* the various $x$ in $A$ were formed (or "given", if atomic).

Thus, at this very same stage $\Sigma$ we can collect into a set just those $x$ in $A$ that are moreover restricted to satisfy $\mathscr{P}[x]$.

**III.2.10 Definition.** Whenever the set term

$$\{x : x \in A \wedge \mathscr{P}\}$$

can be introduced by III.2.9, it is often written more simply as

$$\{x \in A : \mathscr{P}\}$$

□

**III.2.11 Proposition.**

$$\neg U(a), \mathscr{P} \to x \in a \vdash_{\text{ZFC}} (\exists y)\Big(\neg U(y) \wedge (\forall x)(x \in y \leftrightarrow \mathscr{P})\Big)$$

*In words, if $a$ is a set and we know that $\mathscr{P} \to x \in a$, then*

$$Coll_x\mathscr{P}$$

*so we can* introduce *the set (term)* $\{x : \mathscr{P}\}$.

[†] Principle 1, p. 102, is at work here. Recall that we can take or leave this principle. However, we have decided to take it (and hence adopt foundation, later on). It is worth stating that in the absence of Principle 1, a "doctrine on limitation of size" would still effectively argue the "truth" of separation.

*Proof.*

$$\begin{aligned} &(\exists y)\Big(\neg U(y) \land (\forall x)(x \in y \leftrightarrow x \in a \land \mathscr{P})\Big) \\ \leftrightarrow &\Big\langle \text{equivalence theorem and } \mathscr{A} \rightarrow \mathscr{B} \models_{\mathbf{Taut}} \mathscr{A} \leftrightarrow \mathscr{A} \land \mathscr{B} \Big\rangle \\ &(\exists y)\Big(\neg U(y) \land (\forall x)(x \in y \leftrightarrow \mathscr{P})\Big) \end{aligned}$$

Done, since the top line is provable in the presence of the assumption $\neg U(a)$ (separation). □

**III.2.12 Corollary.**

$$\vdash_{\mathrm{ZFC}} \neg U(a) \rightarrow (\forall x)(\mathscr{P} \rightarrow x \in a) \rightarrow (\exists y)\Big(\neg U(y) \land (\forall x)(x \in y \leftrightarrow \mathscr{P})\Big)$$

*Proof.* By the deduction theorem and III.2.11. □

So we can build sets by separation by *restricting* membership to *existing sets*. Unsatisfactory as this may be – since separation only enables us to build "smaller" sets (meaning here subsets) than the ones we have – it gets worse: We have no proof that any set exists yet. We fix this in the next and following sections. One should note that

$$(\exists x)x = x$$

is a theorem of pure logic (axiom $x = x$ followed by the substitution axiom and modus ponens). This says, as far as ZFC is concerned,

$$\text{An object exists!}^{\dagger} \tag{$*$}$$

But what *type* of object? This may well be an atom, so we still have no proof that any *set* exists.

## III.3. The Set of All Urelements; the Empty Set

**III.3.1 Axiom.** *The set of all urelements exists:*

$$Coll_x U(x)$$

**III.3.2 Definition.** We introduce a *new constant*, $M$, into our formal language by the axiom

$$y = M \leftrightarrow \neg U(y) \land (\forall x)(x \in y \leftrightarrow U(x)) \tag{1}$$

† Upon reflection, there is nothing unsettling about pure logic proving that "objects" exist in set theory. This is simply a consequence of our decision – in logic – not to allow empty structures. This decision was also hardwired in the syntactic apparatus of logic.

since

$$\vdash_{\mathrm{ZFC}} (\exists y)\Big(\neg U(y) \wedge (\forall x)(x \in y \leftrightarrow U(x))\Big)$$

by III.3.1. □

That is, we have just introduced the (rather unimaginative) short name $M$ for the set term

$$\{x : U(x)\}$$

since (1) above yields

$$\vdash_{\mathrm{ZFC}} y = M \leftrightarrow y = \{x : U(x)\}$$

and hence, by substitution,

$$\vdash_{\mathrm{ZFC}} M = \{x : U(x)\}$$

**III.3.3 Lemma (Existence of the Empty Set).** $\vdash_{\mathrm{ZFC}} Coll_x \neg x = x$.

*Proof.* By $\vdash \neg x = x \rightarrow x \in M$ and $\vdash_{\mathrm{ZFC}} \neg U(M)$ (the latter by III.3.2) plus III.2.12. □

**III.3.4 Definition (Empty Set).** By III.3.3 we may introduce the set term

$$\{x : \neg x = x\}$$

for the *empty set*. We can then follow this up by the axiom (definition)

$$\emptyset = \{x : \neg x = x\}$$

to introduce (using (9) in III.2.4) the new constant symbol $\emptyset$ for the empty set. □

**III.3.5 Remark.** Referring to 2.6 $(ii)$ and $(iii)$, we see that the intuitive meaning – or "standard semantics" – of $\emptyset$ is the "set with no elements", since it *is* a set, but, moreover, $x \in \emptyset$ is "false" (equivalent to $\neg x = x$) for all $x$. And this is as we hoped it would be (refer also to the discussion in Section II.4).

Syntactically we get the same understanding as follows: By III.2.6 and III.3.4,

$$\vdash_{\mathrm{ZFC}} x \in \emptyset \leftrightarrow \neg x = x$$

Hence, by tautological implication,

$$\vdash_{\mathrm{ZFC}} \neg x \in \emptyset \leftrightarrow x = x$$

Therefore, by the equality axiom $x = x$ and tautological implication,

$$\vdash_{\mathrm{ZFC}} \neg x \in \emptyset$$

or

$$\vdash_{\mathrm{ZFC}} x \notin \emptyset$$

A by-product of the existence of the empty set is a relaxing of the conditions in III.2.11 and III.2.12. We may drop the assumption $\neg U(a)$. Assume $\mathscr{P} \to x \in a$. Now there are two cases (proof by cases). If $\neg U(a)$, then we let III.2.11 or III.2.12 do their thing. If $U(a)$ is the case, then we infer $\neg x \in a$ (III.1.3); hence $x \in a \to x \in \emptyset$ by tautological implication. Another tautological implication gives $\mathscr{P} \to x \in \emptyset$. Since $\vdash_{\mathrm{ZFC}} \neg U(\emptyset)$, we can now invoke III.2.11 to infer $Coll_x \mathscr{P}$. □ ☡

The concluding remark above is worth immortalizing:

**III.3.6 Proposition.** $\vdash_{\mathrm{ZFC}} (\forall x)(\mathscr{P} \to x \in a) \to Coll_x \mathscr{P}$.
*Correspondingly,* $\mathscr{P} \to x \in a \vdash_{\mathrm{ZFC}} Coll_x \mathscr{P}$

**III.3.7 Example.** We saw how to justify the existence (as a formal mathematical object – a set) of a “part of” $M$ in the simple, but very important, case of $\emptyset$. In general, III.2.12 allows us to prove $Coll_x \mathscr{A}$ for any $\mathscr{A}$ for which we know that $\mathscr{A} \to x \in M$ (either as an assumption, or as a provable ZFC fact).

For example, we can show that for any $a$ and $b$ in $M$ we can collect these two elements into a set of “two” elements, *intuitively denoted* by “$\{a, b\}$”. Indeed,

$$\vdash a \in M \wedge b \in M \to x = a \vee x = b \to x \in M \tag{1}$$

In fact,

$$\vdash a \in M \to x = a \to x \in M \tag{2}$$

and

$$\vdash b \in M \to x = b \to x \in M \tag{3}$$

by the Leibniz axiom. Thus, proof by cases (I.4.26, p. 52) helped by $\models_{\mathbf{Taut}}$ gives

$$\vdash x = a \vee x = b \to (a \in M \to x \in M) \vee (b \in M \to x \in M)$$

of which (1) is a tautological consequence.

Thus,

$$\text{if} \quad a \in M \text{ and } b \in M, \quad \text{then} \quad Coll_x(x = a \vee x = b)$$

or, in the formal language (with the "*Coll*" abbreviation),

$$\vdash_{\text{ZFC}} a \in M \wedge b \in M \to Coll_x(x = a \vee x = b) \tag{4}$$

One introduces as usual the set term

$$\{x : x = a \vee x = b\}$$

as a follow-up to (4), and also the new symbol ("set term by listing")

$$\{a, b\}$$

i.e., one defines

$$\{a, b\} = \{x : x = a \vee x = b\} \qquad \square$$

Can we repeat the above for any *sets* $a$ and $b$? That is, is it true that $\vdash_{\text{ZFC}}$ $Coll_x(x = a \vee x = b)$ for any objects $a$ and $b$? In particular, can we say that we can form the (real) sets $\{\{a\}\}$ or $\{\{a\}, \{b\}\}$ in the metatheory? Well, we should hope so, since – intuitively – there is a stage after the stages when $\{a\}$ and $\{b\}$ were built.

However we need a new axiom to formally guarantee this, because all our present axioms are true in the structure with underlying set $\{\emptyset, 1, \{1\}\}$ ($M = \{1\}$ here), but so is

$$(\forall y)\Big(\neg U(y) \to (\forall x)(x \in y \to U(x))\Big)$$

since the members of every set in this structure are atoms. Thus,

$$\text{present set of axioms} + \text{“no set has set elements”} \tag{1}$$

is consistent (cf. I.5.14). Hence

$$\text{present set of axioms} \nvdash \text{“some set has set elements”} \tag{2}$$

Thus, by (2), we cannot prove *yet* that, in particular, a set $\{\{a\}\}$ exists.

One last comment before we leave this section: We choose not to postulate existence of individual urelements, so it may be the case that $M = \emptyset$. This leaves our options open in the sense that we can have the "usual" ZFC (with no urelements) as a special case of our ZFC. We note in this connection that if, instead of having a predicate ($U$) to separate sets from atoms, we adopted a two-sorted language with two "types" of object variables one, say $a, b, c, a', a'', \ldots,$ for sets and one, say, $p, q, p', q'', \ldots,$ for atoms, then

$$\vdash (\exists p)(p = p)$$

would guarantee the existence of atoms, spoiling our present flexibility.

## III.4. Class Terms and Classes

Before moving on towards developing tools for building more complicated sets, we pause to expand our *argot* notation in the interest of achieving more flexibility.

ZFC is about sets and atoms. It does not deal with "higher order" objects such as the Russell collection (which, we have seen, is not a set), and, moreover, its (formal) language has no means of notation for such higher order collections. Nevertheless, much is to be gained in notational uniformity, and hence also in user-friendliness, by allowing *in the metalanguage* the use of symbol sequences of the form $\{x : \mathscr{A}\}$ – called "class terms" – *even if we have no knowledge of*

$$\vdash_{\mathrm{ZFC}} Coll_x \mathscr{A}$$

Indeed, we want to be able to use in formal (syntactic) contexts the "term" $\{x : \mathscr{A}\}$, even if the above may actually fail. Correspondingly, in semantic contexts, the symbol sequence $\{x : \mathscr{A}\}$ serves as a *name* for a real collection $\mathbb{A}$ – that is probably too big to be a set – which $\mathscr{A}$ *first order defines* in the usual sense:[†]

$$x \in \mathbb{A} \quad \text{iff} \quad \mathscr{A}[x] \text{ is true in the standard model of ZFC}$$

The collection that $\mathbb{A}$ names is technically called a *class* (cf. III.4.3). We, of course, simply say "$\mathbb{A}$ is a class".

To protect the innocent I state outright that there is no philosophical significance in restricting attention to first order definable classes. It is not due to a lack of belief in the existence of non-definable classes; rather it is due to a lack of interest in them.

While the intended semantics above is meant to motivate the consideration of (possibly non-set) classes, "real classes" do not intrude into our (*argot*) usage of *class terms*. The latter are employed entirely syntactically. Their use is governed by a "calculus of translations" through which we may introduce or remove class term abbreviations:

**III.4.1 Informal Definition (Class Terms).** For any formula $\mathscr{A}$ of ZFC, the symbol sequence

$$\{x : \mathscr{A}\} \tag{1}$$

is called a *class term*.

[†] In I.5.15 we saw what it means to first order define a *set* in a structure. The notion naturally extends to first order definability of any collection.

We hereby expand the role of this symbol, employing it in the metalanguage for *two* purposes:

(a) If we can show

$$\vdash_{\mathrm{ZFC}} Coll_x \mathscr{A}$$

then we use (1) to *name a (formal) set term* as per III.2.5 – thus, *every set term is also a class term*.

(b) If not, then (1) can still be employed as an *abbreviation of certain formal texts described below* (compare with III.2.6):

$(i)$ $y = \{x : \mathscr{F}\}$ and $\{x : \mathscr{F}\} = y$ each stand for the formal text

$$\neg U(y) \wedge (\forall x)(x \in y \leftrightarrow \mathscr{F})$$

In particular, this reflects the position that a (formal) variable, like $y$, stands for an atom or set (here, a set).

"$=$" in $y = \{x : \mathscr{F}\}$ is not the formal "$=$". We are *not* to parse the informal text "$y = \{x : \mathscr{F}\}$", decomposing it into its ingredients. We take it in its entirety as an alias for the formal text "$\neg U(y) \wedge (\forall x)(x \in y \leftrightarrow \mathscr{F})$". A similar comment applies to informal uses of "$=$", "$\in$", and "$U$" below.

$(ii)$ $\{x : \mathscr{F}\} = \{x : \mathscr{G}\}$ stands for the formula $(\forall x)(\mathscr{F} \leftrightarrow \mathscr{G})$.

$(iii)$ $x \in \{x : \mathscr{F}[x]\}$ stands for the formula $\mathscr{F}[x]$, and (see III.2.7) $x \in \{w : \mathscr{F}[w]\}$ stands for the formula $\mathscr{F}[x]$ (where $w$ is neither free nor bound in $\mathscr{F}[x]$).

$(iv)$ $\{x : \mathscr{F}\} \in \{x : \mathscr{G}\}$ stands for

$$(\exists y)\Big(y = \{x : \mathscr{F}[x]\} \wedge y \in \{x : \mathscr{G}[x]\}\Big)$$

which (with the help of $(i)$ and $(ii)$) becomes

$$(\exists y)\Big(\neg U(y) \wedge (\forall x)(x \in y \leftrightarrow \mathscr{F}[x]) \wedge \mathscr{G}[y]\Big)$$

$(v)$ $\{x : \mathscr{F}\} \in z$ stands for

$$(\exists y)\Big(y = \{x : \mathscr{F}[x]\} \wedge y \in z\Big)$$

which (with the help of $(i)$) becomes

$$(\exists y)\Big(\neg U(y) \wedge (\forall x)(x \in y \leftrightarrow \mathscr{F}[x]) \wedge y \in z\Big)$$

$(vi)$ $U\Big(\{x : \mathscr{F}\}\Big)$ stands for $(\forall x)\neg x = x$. □

**Pause.** So $U\big(\{x : \mathscr{F}\}\big)$ is refutable. Does this prove that $\{x : \mathscr{F}\}$ is a *set*?

**III.4.2 Remark.** (1) Ideally, we should have different notations for the symbol $\{x : \mathscr{F}\}$ according to its status as a name for a set term or not – say, boldface type in the former case, and lightface in the latter. However, it is typographically more expedient to use no such notational distinctions but allow instead the context (established by English text surrounding the use of such terms) to fend off ambiguities.

(2) We already know that for some formulas $\mathscr{A}$, $\vdash_{\mathrm{ZFC}} \neg Coll_x \mathscr{A}$. *Semantically*, for such a formula $\mathscr{A}$, the collection in the metatheory named by the *symbol*

$$\{x : \mathscr{A}[x]\} \tag{$*$}$$

is not a set.

Indeed, using III.4.1($i$) above, we translate the formal "$\vdash_{\mathrm{ZFC}} \neg Coll_x \mathscr{A}$" into the theorem, written in English,

$$\text{"There is no set } y \text{ such that } y = \{x : \mathscr{A}\}\text{"} \tag{$**$}$$

Then, Platonistically, for such a formula $\mathscr{A}$ we know that the collection ($*$) is not a set in the metatheory, since the theorems – such as ($**$) above – of the formal theory are true in the standard model.

For example, we can state that "$\{x : x \notin x\}$ is not a set in the metatheory". The quoted fact is the translation of our formal knowledge that "There is no set $y$ such that $y = \{x : x \notin x\}$", or in full formal armor[†]

$$\vdash \neg(\exists y)\Big(\neg U(y) \wedge (\forall x)(x \in y \leftrightarrow x \notin x)\Big) \qquad \square$$

For the semantic and informal side of things and for future reference we state:

**III.4.3 Informal Definition (Real Classes).** A (real) *class* is a collection that is first order definable in the standard structure (in the language of ZFC). Specifically, the class term

$$\{x : \mathscr{A}(x, z_1, \ldots, z_n)\} \tag{1}$$

names a real collection, also denoted by $\mathbb{A}(z_1, \ldots, z_n)$, that is first order defined by the formula $\mathscr{A}(x, z_1, \ldots, z_n)$. That is, for any choice of values for the

[†] The reader will recall that this is a fact of logic, whence just "$\vdash$".

*parameters* $z_1, \ldots, z_n$,

$$x \in \mathbb{A}(z_1, \ldots, z_n) \quad \text{iff} \quad \mathscr{A}(x, z_1, \ldots, z_n) \text{ is true}$$

If, for some choice of closed terms $\vec{t}_n$, $\vdash_{\mathrm{ZFC}} Coll_x \mathscr{A}(x, t_1, \ldots, t_n)$, then $\mathbb{A}(\vec{t}_n)$ denotes a real set; otherwise it denotes a *non*-set class, called a *proper class*.

For the sake of convenience we will use "blackboard bold" capital letters as short *names* of classes; e.g., $\mathbb{A}$ abbreviates the class term $\{x : \mathscr{A}\}$ and we may write, using the metalinguistic "=",

$$\mathbb{A} = \{x : \mathscr{A}\}$$

These names are *metavariables*.† We will normally adopt the general convention of naming a class term by the blackboard bold version of the same letter that denotes the defining formula.

For example, $\mathbb{A} = \mathbb{B}$ is short for $\{x : \mathscr{A}\} = \{x : \mathscr{B}\}$, $\mathbb{A} \in \mathbb{B}$ is short for $\{x : \mathscr{A}\} \in \{x : \mathscr{B}\}$, etc. – expressions which can be translated into the formal language using III.4.1. □

**III.4.4 Remark.** (1) Worth repeating: Class *terms* are just *symbols* that name certain entities of our intuition, namely, classes. We will often abuse terminology and say "let $\{x : \mathscr{A}\}$ *be* a class" rather than "let $\{x : \mathscr{A}\}$ *name* a class", just as one may say (under the assurance of $\vdash_{\mathrm{ZFC}} Coll_x \mathscr{A}$) "let $\{x : \mathscr{A}\}$ *be* a *set*". Properly speaking, a *class term* is an *syntactic* object, while a *class* is a "real" object.

(2) What class terms and classes do for us is analogous to what number theory *argot* does for us in Peano arithmetic (**PA**). Such *argot* allows us to write, e.g., the easily understandable informal text

$$\vdash_{\mathbf{PA}} \text{ every } n > 1 \text{ has a prime divisor}$$

instead of

$$\begin{aligned}\vdash_{\mathbf{PA}} (\forall n)\Big(n > 1 \rightarrow (\exists x)(\exists y)\big(n = x \times y \wedge \\ x > 1 \wedge (\forall m)(\forall r)(x = m \times r \rightarrow m = 1 \vee m = x)\big)\Big)\end{aligned}$$

† We note that $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are already reserved for the natural numbers, integers, rational numbers, reals, and complex numbers. These are metalinguistic constants. Besides, we have already called the Russell proper class "$R$", and later we will use "On" and "Cn" for certain proper classes. This does not conflict with the blackboard bold notation for indeterminate class names.

In particular, in the context of class terms one can readily replace "stands for" by "$\leftrightarrow$" to write – for example – something like (cf. III.4.1($i$))

$$\vdash y = \{x : \mathscr{F}\} \leftrightarrow \neg U(y) \wedge (\forall x)(x \in y \leftrightarrow \mathscr{F}) \tag{$*$}$$

We can obtain (an absolute) proof of ($*$) by starting with the tautology

$$\neg U(y) \wedge (\forall x)(x \in y \leftrightarrow \mathscr{F}) \leftrightarrow \neg U(y) \wedge (\forall x)(x \in y \leftrightarrow \mathscr{F})$$

and then *abbreviating* the left hand side, "$\neg U(y) \wedge (\forall x)(x \in y \leftrightarrow \mathscr{F})$", by "$y = \{x : \mathscr{F}\}$" using the translation rule III.4.1($i$).

(3) Every "real" set named by some formal term $t$ is a class, since (by III.2.8)

$$y = \{x : x \in y\}$$

and hence

$$t = \{x : x \in t\}$$

by substitution.[†] □

**III.4.5 Example.**

(a)

$$y = \mathbb{A} \tag{1}$$

(or $\mathbb{A} = y$) is very short text for $y = \{x : \mathscr{A}\}$, which in turn is short for (III.4.1($i$))

$$\neg U(y) \wedge (\forall x)(x \in y \leftrightarrow \mathscr{A}) \tag{2}$$

Thus, whenever we claim that we can prove (1), we really mean that we can prove (2). In particular, such a proof yields also a proof that

(i) $Coll_x \mathscr{A}$ (by substitution axiom and modus ponens); hence $\{x : \mathscr{A}\}$ is (i.e., can be introduced as) a *set term*; thus, $\mathbb{A}$ is (denotes) a *set*.

**Pause.** What is all this roundabout argument for? Why don't we just say, "$\mathbb{A}$, a class, equals a set $y$.[‡] Therefore, it is itself a set"?

(ii) $x \in y \leftrightarrow \mathscr{A}$.

(b)

$$\mathbb{A} \in \mathbb{B} \tag{3}$$

[†] Without loss of generality, $x$ is not free in $t$.

[‡] Recall the convention on variable names. $y$ names a set or atom, but it is not an atom here.

is very short for

$$\{x : \mathscr{A}\} \in \{x : \mathscr{B}[x]\} \tag{4}$$

which is short for (III.4.1($iv$))

$$(\exists y)\Big(\neg U(y) \wedge (\forall x)(x \in y \leftrightarrow \mathscr{A}) \wedge \mathscr{B}[y]\Big) \tag{5}$$

Now, to say that we have a proof of (3) (or that we *assume* (3)) is to say that we have a proof of (5) (or that we *assume* (5)). From the latter, tautological implication along with $\exists$-monotonicity (I.4.23) yields

$$(\exists y)\Big(\neg U(y) \wedge (\forall x)(x \in y \leftrightarrow \mathscr{A})\Big)$$

that is, $Coll_x \mathscr{A}$. In words, "(3) implies that $\mathbb{A}$ is a set". This corresponds well with our intention that class members are sets or atoms. Here $\mathbb{A}$, being a collection, is not an atom. □

**III.4.6 Example.** By III.4.1($i$, $ii$), if $y = \mathbb{A}$ then $\mathbb{A} = y$, and if $\mathbb{A} = \mathbb{B}$ then $\mathbb{B} = \mathbb{A}$.[†] Moreover, $\mathbb{A} = \mathbb{A}$ is a theorem of logic, since $\vdash \mathscr{A} \leftrightarrow \mathscr{A}$.

Transitivity of this (informal) class equality is also guaranteed, from $\mathscr{A} \leftrightarrow \mathscr{B}, \mathscr{B} \leftrightarrow \mathscr{C} \models_{\textbf{Taut}} \mathscr{A} \leftrightarrow \mathscr{C}$ and Definition III.4.1($ii$). □

**III.4.7 Informal Definition (Subclass and Superclass of a Class).** The notation $\mathbb{A} \subseteq \mathbb{B}$ stands for

$$(\forall x)(x \in \mathbb{A} \rightarrow x \in \mathbb{B})$$

and is pronounced "$\mathbb{A}$ is a *subclass* of $\mathbb{B}$", or "$\mathbb{B}$ is a *superclass* of $\mathbb{A}$". We can also write $\mathbb{B} \supseteq \mathbb{A}$.

$\mathbb{A} \subset \mathbb{B}$ (also $\mathbb{B} \supset \mathbb{A}$) stands for $\mathbb{A} \subseteq \mathbb{B} \wedge \neg \mathbb{A} = \mathbb{B}$ and is read "$\mathbb{A}$ is a *proper*[‡] subclass of $\mathbb{B}$" (also "$\mathbb{B}$ is a proper superclass of $\mathbb{A}$").

If $\mathbb{A} \subseteq \mathbb{B}$ and $\mathbb{A}$ is a set we say, as before, that $\mathbb{A}$ is a *subset* of $\mathbb{B}$. □

We have at once:

**III.4.8 Proposition.**

($i$) $\vdash \mathbb{A} \subseteq \mathbb{B} \leftrightarrow (\forall x)(\mathscr{A} \rightarrow \mathscr{B})$
($ii$) $\vdash \mathbb{A} \subseteq \mathbb{B} \wedge \mathbb{B} \subseteq \mathbb{A} \leftrightarrow \mathbb{A} = \mathbb{B}$

[†] Indeed, $\vdash \mathbb{A} = \mathbb{B} \leftrightarrow \mathbb{B} = \mathbb{A}$ translates to the formal $\vdash (\mathscr{A} \leftrightarrow \mathscr{B}) \leftrightarrow (\mathscr{B} \leftrightarrow \mathscr{A})$.

[‡] This "proper" qualifies "subclass", not "class". Thus a proper subclass could still be a *set*.

*Proof.* $(i)$: $\mathbb{A} \subseteq \mathbb{B} \leftrightarrow (\forall x)(x \in \mathbb{A} \rightarrow x \in \mathbb{B})$ is a tautology "$\mathscr{G} \leftrightarrow \mathscr{G}$" by III.4.7. We use III.4.1 to eliminate "$x \in \cdots$"; thus $\vdash \mathbb{A} \subseteq \mathbb{B} \leftrightarrow (\forall x)(\mathscr{A} \rightarrow \mathscr{B})$.

$(ii)$: We translate $(ii)$ using $(i)$ that we have just verified, and III.4.1:

$$(\forall x)(\mathscr{A} \rightarrow \mathscr{B}) \wedge (\forall x)(\mathscr{B} \rightarrow \mathscr{A}) \leftrightarrow (\forall x)(\mathscr{A} \leftrightarrow \mathscr{B})$$

Distribution of $\forall$ over $\wedge$ to the left of the first $\leftrightarrow$, along with the tautology theorem and equivalence theorem, shows that the above is a theorem of pure logic. □

**Pause.** So, does $(ii)$ above prove extensionality?

**III.4.9 Example.** What can we learn from $\vdash_{\text{ZFC}} \neg U(y) \wedge \mathbb{A} \subseteq y$? Well, III.2.8, III.4.7 and III.4.8 allow us to translate the above into

$$\vdash_{\text{ZFC}} \neg U(y) \wedge (\forall x)(\mathscr{A} \rightarrow x \in y)$$

By III.2.12 and modus ponens we get

$$\vdash_{\text{ZFC}} Coll_x \mathscr{A}$$

That is, $\mathbb{A}$ is a set. Another way to say all this is

$$\vdash_{\text{ZFC}} \neg U(y) \wedge \mathbb{A} \subseteq y \rightarrow Coll_x \mathscr{A}$$ □

The above is worth immortalizing, in English:

**III.4.10 Proposition (Class Form of Separation).** *Any subclass of a set is a set.*

**III.4.11 Example.** We translate the very common informal text "$\mathbb{A} \neq \emptyset$": first, into $\neg(\{x : \mathscr{A}\} = \emptyset)$, and next, taking $\vdash_{\text{ZFC}} \emptyset = \{x : \neg x = x\}$ into account,

$$\neg(\forall x)(\mathscr{A} \leftrightarrow \neg x = x)$$

that is,

$$(\exists x)\neg(\mathscr{A} \leftrightarrow \neg x = x) \tag{1}$$

But

$$\models_{\textbf{Taut}} \neg(\mathscr{Q} \leftrightarrow \mathscr{P}) \leftrightarrow (\mathscr{Q} \leftrightarrow \neg\mathscr{P})$$

Thus (1) is provably (within pure logic) equivalent to

$$(\exists x)(\mathscr{A} \leftrightarrow x = x) \tag{2}$$

by the equivalence theorem.

Since $x = x$ is a logical axiom, (2) is provably (within pure logic) equivalent to

$$(\exists x)\mathscr{A}$$

This is the translation of $\mathbb{A} \neq \emptyset$. Correspondingly, $\mathbb{A} = \emptyset$ translates to $\neg(\exists x)\mathscr{A}$.

A class that equals $\emptyset$ is called, of course, *empty*. However, many authors also use the term *void*, or *null*, class if $\mathbb{A} = \emptyset$, and correspondingly, *non-void*, or *non-null*, if $\mathbb{A} \neq \emptyset$. □

**III.4.12 Informal Definition (Class Union, Intersection, and Difference).** We introduce the following *metalinguistic* abbreviations:

(a) $\mathbb{A} \cup \mathbb{B}$, pronounced *the union of* $\mathbb{A}$ *and* $\mathbb{B}$, abbreviates $\{x : x \in \mathbb{A} \vee x \in \mathbb{B}\}$.
(b) $\mathbb{A} \cap \mathbb{B}$, pronounced *the intersection of* $\mathbb{A}$ *and* $\mathbb{B}$, abbreviates $\{x : x \in \mathbb{A} \wedge x \in \mathbb{B}\}$. If $\mathbb{A} \cap \mathbb{B} = \emptyset$, then we say that $\mathbb{A}$ and $\mathbb{B}$ are *disjoint*.
(c) $\mathbb{A} - \mathbb{B}$, pronounced *the difference of* $\mathbb{A}$ *and* $\mathbb{B}$ *in that order*, abbreviates $\{x : x \in \mathbb{A} \wedge x \notin \mathbb{B}\}$. □

Some authors use "$\sim$" or even "\" for difference instead of "$-$".

**III.4.13 Example.** $\nvdash \mathbb{A} - \mathbb{B} = \mathbb{B} - \mathbb{A}$. Indeed, if $a \neq b$,

$$\vdash \{x : x = a\} - \{x : x = a \vee x = b\} = \emptyset$$

while

$$\vdash \{x : x = a \vee x = b\} - \{x : x = a\} = \{x : x = b\}$$ □

It is immediate that

**III.4.14 Proposition.** *If* $\mathbb{A}$ *or* $\mathbb{B}$ *is a set, then so is* $\mathbb{A} \cap \mathbb{B}$. *If* $\mathbb{A}$ *is a set, then so is* $\mathbb{A} - \mathbb{B}$.

*Proof.* By III.4.10 and (1)–(3) below:

(1) $\vdash \mathbb{A} \cap \mathbb{B} \subseteq \mathbb{A}$
(2) $\vdash \mathbb{A} \cap \mathbb{B} \subseteq \mathbb{B}$
(3) $\vdash \mathbb{A} - \mathbb{B} \subseteq \mathbb{A}$

To see why (1) holds, we eliminate class terms:

$$(\forall x)(\mathscr{A} \wedge \mathscr{B} \to \mathscr{A})$$

The above is provable in pure logic. Similarly for (2). Also, (3) translates to

$$\vdash (\forall x)(\mathscr{A} \wedge \neg \mathscr{B} \rightarrow \mathscr{A}) \qquad \Box$$

Associativity of each of ∪ and ∩ (Exercises III.19 and III.20) allows one to omit brackets and write "$\mathbb{A} \cap \mathbb{B} \cap \mathbb{C}$" or, by recursion on $n \in \mathbb{N}$,[†]

**III.4.15 Informal Definition.**

$$\bigcup_{i=1}^{1} \mathbb{A}_i \text{ stands for } \mathbb{A}_1$$

$$\bigcup_{i=1}^{n+1} \mathbb{A}_i \text{ stands for } \Big(\bigcup_{i=1}^{n} \mathbb{A}_i\Big) \cup \mathbb{A}_{n+1}$$

and

$$\bigcap_{i=1}^{1} \mathbb{A}_i \text{ stands for } \mathbb{A}_1$$

$$\bigcap_{i=1}^{n+1} \mathbb{A}_i \text{ stands for } \Big(\bigcap_{i=1}^{n} \mathbb{A}_i\Big) \cap \mathbb{A}_{n+1}$$

The symbols "$\bigcup_{i=1}^{n}$" and "$\bigcap_{i=1}^{n}$" are also written as "$\bigcup_{1 \le i \le n}$" and "$\bigcap_{1 \le i \le n}$" respectively.

In a moment of weakness one may find oneself writing "$\mathbb{A}_1 \cup \cdots \cup \mathbb{A}_n$" and "$\mathbb{A}_1 \cap \cdots \cap \mathbb{A}_n$" respectively. □

**III.4.16 Remark (Formal ∩ and Difference).** We cannot prove similar results (to those contained in III.4.14) for union *yet*. We will have to wait for the axiom of union.

Note that in a classless approach one could carry out Definition III.4.12 and Proposition III.4.14 as follows:

For the definition, for example of "∩", one would introduce a new 2-ary (binary) *function* symbol, "∩", *formally* by the defining axiom

$$x \cap y = z \leftrightarrow \neg U(z) \wedge (\forall w)(w \in z \leftrightarrow w \in x \wedge w \in y) \qquad (i)$$

$(i)$ is legitimate because $\vdash_{\mathrm{ZFC}} Coll_w(w \in x \wedge w \in y)$. Indeed,

$$\models_{\textbf{Taut}} w \in x \wedge w \in y \rightarrow w \in x \qquad (ii)$$

[†] Recall that definitions, both formal and informal ones, are effected in the metatheory, where we have tools such as natural numbers, induction, and recursion over $\mathbb{N}$.

Thus (by III.3.6)

$$\vdash_{\mathrm{ZFC}} \mathit{Coll}_w(w \in x \wedge w \in y) \tag{$iii$}$$

We note that $x \cap y$ makes sense *formally* even when one or both of $x$ and $y$ are atoms, whereas the informal $\cap$ was defined only for classes.[†] The defining axiom $(i)$ and III.1.3 prove

$$\vdash_{\mathrm{ZFC}} U(x) \to x \cap y = \emptyset$$

and

$$\vdash_{\mathrm{ZFC}} U(y) \to x \cap y = \emptyset$$

Similarly, difference would be introduced formally by

$$x - y = z \leftrightarrow \neg U(z) \wedge (\forall w)(w \in z \leftrightarrow w \in x \wedge \neg w \in y) \tag{$v$}$$

The proof of the legitimacy of $(v)$ is left to the reader. Note that here too $x - y$, *formally*, makes sense for atom "arguments". Moreover, we have the "pathological" special cases

$$\vdash_{\mathrm{ZFC}} U(x) \to x - y = \emptyset$$

and

$$\vdash_{\mathrm{ZFC}} \neg U(x) \to U(y) \to x - y = x$$

So much for the formal "$\cap$" and "$-$". Of course, the defining axiom for the formal "$\cup$" will still have to wait for the union axiom.

Since we would have sooner or later to extend the formal "$\cap$", "$\cup$", "$-$" (recorded below) to the class versions to use in our *argot*, we decided to introduce these symbols as (informal) abbreviations to begin with (as is done in, e.g., Levy (1979)). □

**III.4.17 Definition.** For the record, we introduce the 2-ary function symbols "$\cap$" and "$-$" *formally* to our language, and add the defining axioms $(i)$ and $(v)$ of III.4.16 to our theory.

The context will easily tell in each use whether we are employing these symbols formally, or as abbreviations as per III.4.12. □

[†] It is normal practice in a first order language to insist that function symbols stand for *totally defined* or *total* functions, upon interpretation. Thus it is appropriate that $\cap$ and $-$ are defined on all objects.

**III.4.18 Informal Definition (the Universe; the Universe of All Sets).** We introduce the following abbreviations for the class terms $\{x : x = x\}$ and $\{x : \neg U(x)\}$:

$$\mathbb{U}_M = \{x : x = x\}$$

and

$$\mathbb{V}_M = \{x : \neg U(x)\}$$

In the "real" sense, i.e., semantically, $\mathbb{U}_M$ is the universe of all objects set theory is about, while $\mathbb{V}_M$ is the universe of all *sets*, i.e., the atoms are not included in $\mathbb{V}_M$ (they are used however to build sets). □

The following is immediate.

**III.4.19 Proposition.**

(1) $\mathbb{U}_M$ *is a proper class.*
(2) $\vdash_{\mathrm{ZFC}} \mathbb{U}_M = \mathbb{V}_M \cup M$.

*Proof.* (1): Indeed, $R$, the Russell class, satisfies $\vdash R \subseteq \mathbb{U}_M$, since $\vdash x \notin x \rightarrow x = x$. If $\mathbb{U}_M$ were a set, then so would $R$ be by III.4.10.

(2): $\mathbb{U}_M = \mathbb{V}_M \cup M$ translates to (by III.3.2, III.4.1($ii$) and III.4.12)

$$x = x \leftrightarrow \neg U(x) \vee U(x)$$ □

☡ Once we have the union axiom (which says that the union of two sets is a set), we will obtain that $\mathbb{V}_M$ is a proper class too (by (2) above and III.3.1).[†] ☡

☡☡ **III.4.20 Remark (Alternate Universes).** (1) The symbol $\mathbb{U}_N$ will, in general, denote the class of *all sets and atoms* built from the *arbitrarily chosen* initial set of atoms $N \subseteq M$. If $N = \emptyset$, then we simply write $\mathbb{U}$ rather than $\mathbb{U}_\emptyset$. The reader will note that while $\mathbb{U}_M$ (where $M$ is the set of *all* urelements) is trivially given by the class term $\{x : x = x\}$, it takes, a glimpse forward (to Chapter VI) to show that $\mathbb{U}_N$ *can* also be defined by a class term – as we require for all classes – for any $N \subseteq M$. One way to do this is using the *support function*, "*sp*" (see VI.2.34), namely $\mathbb{U}_N = \{x : sp(x) \subseteq N\}$. The latter says, "an object is in $\mathbb{U}_N$ iff when we disassemble it all the way down to its constituent urelements, *all* these urelements are in $N$".

[†] Note that if $M \neq \emptyset$ then $M \subseteq R$; thus $R \nsubseteq \mathbb{V}_M$.

Similarly, we can define the class of all sets whose construction is based on the urelements in $N \subseteq M$, $\mathbb{V}_N$. We write just $\mathbb{V}$ for $\mathbb{V}_\emptyset$. We note that $\mathbb{V}_N$ is given by the class term $\{x : \neg U(x) \wedge sp(x) \subseteq N\}$.

(2) In many elementary developments of the subject one often works within a "reference set", or "relative universe", $X$ (a set), and the sets of interest are subsets or members of $X$. With this understanding, one would write "$-A$" or "$\overline{A}$" for $X - A$ (where $A \subseteq X$, and therefore $A$ is a set) and call "$-A$" *the complement* of $A$ (with respect to $X$). Note that for any set $A \in \mathbb{U}_N$, $\mathbb{U}_N - A$ (for any $N \subseteq M$) is a proper class (Exercise III.21); thus we will have little use for complements. It is the difference (most of the time of sets, rather than classes) that we will have use for. □ ☡☡

We note our intention to use informal class notation extensively. Therefore, it is important to remember at all times that ZFC set theory *does not admit* (proper) *classes as formal objects of study*.[†]

Invariably, there is nothing that we can say with the help of a class term $\{x : \mathscr{A}(x)\}$ that cannot also be said – with a lot more effort and a lot less intuitive transparency – by just using the formula $\mathscr{A}(x)$ instead (e.g., Bourbaki (1996b) and Shoenfield (1967) do not employ classes at all). Definition III.4.1 will be used as a tool to eliminate class terms in order to go back to the formal language of set theory – whenever such caution is necessary (notably in the introduction of axioms).

## III.5. Axiom of Pairing

Consider now any two sets $A$ and $B$. Say the first was built at stage $\Sigma_A$ and the second at stage $\Sigma_B$. We have no difficulty imagining that a stage $\Sigma$ exists *following* both these stages. By Principle 0 (p. 102), at stage $\Sigma$ we can built *any* set whose elements are available. In particular $A$ and $B$ are available; thus a set that contains exactly $A$ and $B$ exists. However, the axiom that flows from this discussion – the axiom for *pairing* – will have a simpler form if we allow the possibility of additional members, beyond $A$ and $B$, in the set asserted to exist.

**III.5.1 Axiom (Unordered Pair).** *For any atoms or sets $a$ and $b$ there is a set $c$ such that $a \in c$ and $b \in c$. Or, stated in the formal language,*

$$(\exists z)(a \in z \wedge b \in z)$$

[†] Other axiomatizations of set theory, originating with Gödel and Bernays, admit (proper) classes as *formal objects* of study. See for example Monk (1969).

*or still (universal closure of the above)*

$$(\forall x)(\forall y)(\exists z)(x \in z \wedge y \in z)$$

**III.5.2 Remark.** By III.1.3, $\vdash_{\mathrm{ZFC}} a \in z \rightarrow \neg U(z)$. Thus, by tautological implication $\vdash_{\mathrm{ZFC}} a \in z \wedge b \in z \leftrightarrow \neg U(z) \wedge a \in z \wedge b \in z$. The equivalence theorem then gives

$$\vdash_{\mathrm{ZFC}} (\exists z)(\neg U(z) \wedge a \in z \wedge b \in z)$$

Thus the object $z$ guaranteed to exist in III.5.1 is a set, as expected. □

**III.5.3 Proposition.** $\vdash_{\mathrm{ZFC}} (\forall a)(\forall b) Coll_x(x = a \vee x = b)$.

*Proof.* It suffices to prove

$$\vdash_{\mathrm{ZFC}} Coll_x(x = a \vee x = b)$$

We have

(1) $(\exists z)(a \in z \wedge b \in z)$ $\quad\big\langle$III.5.1$\big\rangle$

(2) $a \in A \wedge b \in A$ $\quad\big\langle$added; $A$ is a new constant$\big\rangle$

(3) $a \in A$ $\quad\big\langle$(2) plus taut. implic.$\big\rangle$

(4) $b \in A$ $\quad\big\langle$(2) plus taut. implic.$\big\rangle$

(5) $\neg U(A)$ $\quad\big\langle$(3) plus III.1.3 plus MP$\big\rangle$

(6) $x = a \rightarrow (x \in A \leftrightarrow a \in A)$ $\quad\big\langle$Leibniz axiom$\big\rangle$

(7) $x = b \rightarrow (x \in A \leftrightarrow b \in A)$ $\quad\big\langle$Leibniz axiom$\big\rangle$

(8) $x = a \rightarrow x \in A$ $\quad\big\langle$(6) and (3) and taut. impl.$\big\rangle$

(9) $x = b \rightarrow x \in A$ $\quad\big\langle$(7) and (4) and taut. impl.$\big\rangle$

(10) $x = a \vee x = b \rightarrow x \in A$ $\quad\big\langle$(8) and (9) and taut. impl.$\big\rangle$

(11) $Coll_x(x = a \vee x = b)$ $\quad\big\langle$(10) and (5) and III.2.11$\big\rangle$ □

**III.5.4 Corollary.** $\vdash_{\mathrm{ZFC}} Coll_x(x = a)$.

*Proof.* See the proof above, and use (5) plus (8) and III.2.11. Alternatively (without referring to the proof), by $\models_{\mathbf{Taut}} x = a \leftrightarrow x = a \vee x = a$. □

**III.5.5 Definition (Pairs and Singletons).** The above proposition and its corollary allow the *formal* introduction of the *set* terms

$$\{x : x = a \lor x = b\} \tag{1}$$

and

$$\{x : x = a\} \tag{2}$$

We also introduce the terms $\{a, b\}$ (*unordered pair*) and $\{a\}$ (*singleton*) by the formal definitions (cf. III.2.4)

$$\{a, b\} = \{x : x = a \lor x = b\}$$

and

$$\{a\} = \{x : x = a\} \qquad \square$$

**III.5.6 Remark (Denoting Sets by Listing).** We say that $\{a, b\}$ and $\{a\}$ denote sets by *explicit listing* of their members. We note that the informal notation $\mathbb{N} = \{0, 1, 2, \ldots\}$ does *not* denote a set by explicit listing (in the metatheory). Such notation is only possible for what we intuitively understand as "finite" sets. The "$\ldots$" indicates our inability to conclude the listing and hints at a "rule", or understanding, of how to obtain more elements. Such understanding depends on the context (in the case of $\mathbb{N}$, just add 1 to get the next member). □

**III.5.7 Proposition.** $\vdash_{\mathrm{ZFC}} \{a, b\} = \{b, a\}$ *and* $\vdash_{ZFC} \{a\} = \{a, a\}$.

*Proof.* By III.2.6, commutativity of $\lor$, and *idempotency* of $\lor$ (i.e., $\models_{\mathbf{Taut}} \mathscr{A} \leftrightarrow \mathscr{A} \lor \mathscr{A}$). □

**III.5.8 Remark.** (i) Why "$\vdash_{\mathrm{ZFC}}$" rather than just "$\vdash$" above? That is because $\{a, b\}$ and $\{a\}$ were *formally* introduced as terms (sets) in III.5.5. Their introduction necessitated the prior proof in (our present fragment of) ZFC of the formulas $Coll_x(x = a \lor x = b)$ and $Coll_x(x = a)$. As far as the *class terms* $\{x : x = a \lor x = b\}$ and $\{x : x = a\}$ are concerned, we have[†]

$$\vdash \{x : x = a \lor x = b\} = \{x : x = b \lor x = a\} \tag{1}$$

and

$$\vdash \{x : x = a\} = \{x : x = a \lor x = a\} \tag{2}$$

[†] Cf. III.4.1 regarding the use of the unbracketed "=" in (1) and (2).

by III.4.1, since the above simply abbreviate

$$\vdash x = a \lor x = b \leftrightarrow x = b \lor x = a \tag{3}$$

and

$$\vdash x = a \leftrightarrow x = a \lor x = a \tag{4}$$

Thus, (1) and (2) are just stating the tautologies in (3) and (4), while Proposition III.5.7 states much more in between the lines, in particular that $\{a, b\}$ and $\{a\}$ are sets.

*If* we had introduced the pair and singleton as abbreviations of the respective *class terms* instead,[†] then the above proposition would be provable in pure logic – for it would be just stating (3) and (4) – and whether or not the terms referenced are sets would be a separate issue.

This remark was necessitated by our decision not to differentiate the notations for set terms and class terms.

(ii) Proposition III.5.7 is popularized in naïve set theory by saying "when we list the elements of a set explicitly, multiplicity or order of elements does not matter". □

**III.5.9 Remark (Relaxing the Proof Style).** It would be counterproductive to introduce a rich *argot* towards the simplification of formal texts on one hand, while on the other hand we continue to offer extremely detailed formal proofs such as the one for III.5.3. Well, we do not have to be that formal always, nor can we afford to be so when our arguments get more involved. We will frequently relax the proof style to shorten proofs. This relaxing will invariably use shorthand tools such as English text, class terms, and a judicious omission of (proof) details.

For example, a relaxed version of the proof of III.5.3 would read like this: Let $a$ and $b$ be any objects (i.e., sets or urelements). Let us denote by $c$ any set (asserted to exist in III.5.1) such that $a \in c$ and $b \in c$ [this combines steps (1)–(5) of the formal proof]. Thus $\{x : x = a \lor x = b\} \subseteq c$; hence $\{x : x = a \lor x = b\}$ (denotes) is a set by separation (III.4.10) [the obvious steps (6)–(10) were just compacted to (10)]. □

While the axiom of pairing is not provable from the axioms that we had at our disposal prior to its introduction (see p. 133), it becomes provable once (an

[†] This is how it is often done; e.g., Levy (1979).

appropriate version of) *collection* and *power set* axioms are introduced (see Exercises III.15 and III.16).

## III.6. Axiom of Union

How about the classes $\{x : x = a \vee x = b \vee x = c\}$ and $\{x : x = a \vee x = b \vee x = c \vee x = d\}$ – for short, $\{a, b, c\}$ and $\{a, b, c, d\}$ – where $a, b, c, d$ are arbitrary objects? Are these sets?

Of course, we could invoke Principle 0 (p. 102) again, and show that these classes are sets indeed. However, it is not fitting an axiomatic approach to go back to this *metamathematical* principle all the time. It is more elegant – and safer – to have just one axiom that will imply that all such objects are sets. What we have in mind is something more powerful than an endless sequence of axioms for (unordered) triple, quadruple, etc.

We already know that $\{a, b\}$, $\{c, d\}$, and $\{c\}$ are sets. Then, applying pairing again, the following are sets too:

$$\big\{\{a, b\}, \{c\}\big\} \tag{1}$$

and

$$\big\{\{a, b\}, \{c, d\}\big\} \tag{2}$$

What we need is the ability to remove the level of braces just below the outermost, to obtain the (unordered) triple (from (1)) and quadruple (from (2)). In essence, we want to know that, in particular, $\{a, b\} \cup \{c\}$ and $\{a, b\} \cup \{c, d\}$ are sets.

We will address this immediately, but in somewhat more general setting. First, we will define the operation that removes the "top level" of braces of all non-atomic members of a class. To this end, and in all that follows in this volume, we will benefit from a notational device. We often use *bounded quantification* in set theory, i.e., "there is an $x$ *in* $A$ such that ... " and "for all $x$ *in* $A$ it follows that ... ".

**III.6.1 Informal Definition (Bounded Quantification).** The notations $(\exists x \in \mathbb{A})\mathscr{F}$ and $(\forall x \in \mathbb{A})\mathscr{F}$ are short forms of $(\exists x)(x \in \mathbb{A} \wedge \mathscr{F})$ and $(\forall x)(x \in \mathbb{A} \rightarrow \mathscr{F})$ respectively. □

**III.6.2 Example.** We can easily verify that De Morgan's laws hold for bounded quantification, i.e.,

$$\vdash (\exists x \in \mathbb{A})\mathscr{F} \leftrightarrow \neg(\forall x \in \mathbb{A})\neg\mathscr{F}$$

Indeed,

$$
\begin{aligned}
& \neg(\forall x \in \mathbb{A})\neg\mathscr{F} \\
\leftrightarrow\; & \Big\langle \text{by III.6.1} \Big\rangle \\
& \neg(\forall x)(x \in \mathbb{A} \to \neg\mathscr{F}) \\
\leftrightarrow\; & \Big\langle \text{equiv. theorem} \Big\rangle \\
& \neg(\forall x)(\neg x \in \mathbb{A} \vee \neg\mathscr{F}) \\
\leftrightarrow\; & \Big\langle \text{“}\forall\text{-De Morgan”} \Big\rangle \\
& (\exists x)\neg(\neg x \in \mathbb{A} \vee \neg\mathscr{F}) \\
\leftrightarrow\; & \Big\langle \text{“}\vee\text{-De Morgan” and equiv. theorem} \Big\rangle \\
& (\exists x)(x \in \mathbb{A} \wedge \mathscr{F}) \\
\leftrightarrow\; & \Big\langle \text{by III.6.1} \Big\rangle \\
& (\exists x \in \mathbb{A})\mathscr{F} \qquad \square
\end{aligned}
$$

**III.6.3 Informal Definition (Union of a Class; Union of a Family of Sets).** Let $\mathbb{A}$ be a class. The symbol $\bigcup \mathbb{A}$ is an abbreviation of the class term $\{x : (\exists y \in \mathbb{A})x \in y\}$. We read $\bigcup \mathbb{A}$ as *the union of all the sets in* $\mathbb{A}$.

If $\mathbb{A}$ contains no atoms, then it is called a *family of sets*, and $\bigcup \mathbb{A}$ is *the union of the family* $\mathbb{A}$. □

**III.6.4 Remark.** Let $\mathbb{A} = \{x : \mathscr{A}[x]\}$. We have a number of variations in the notation for $\bigcup \mathbb{A}$, namely, $\bigcup_{x \in \mathbb{A}} x$ or $\bigcup\{x : \mathscr{A}[x]\}$ or $\bigcup_{\mathscr{A}[x]} x$. In any case, after we eliminate class notation, all these notations stand for the class term $\{x : (\exists y)(\mathscr{A}[y] \wedge x \in y)\}$. □

**III.6.5 Example.** $\bigcup \big\{\#, \{|\}, \{1, \{2\}\}\big\} = \big\{|, 1, \{2\}\big\}$, where “#”, “|”, “1”, “2” are names for atoms. So, in the result of the union, “loose atoms” are lost. □

Let now $A$ be a set, and consider $\bigcup A$, that is, $\{x : (\exists y \in A)x \in y\}$. Let $A$ be formed at stage $\Sigma$. Then each $y \in A$ must be available before $\Sigma$, and since $x \in y$ for each $x$ that we collect in $\bigcup A$, *a fortiori*, $x$ is available before $\Sigma$. It follows that $\bigcup A$ itself can be built at $\Sigma$ as a set, so it *is* a set. As in the case of pairing, we state the following axiom of union in a “weak” form. It asserts the existence of a set that contains the union as a subclass. This, by III.4.10, makes the union a set.

**III.6.6 Axiom (Union).**

$$(\exists z)(\forall x)(\forall y)(x \in y \wedge y \in A \rightarrow x \in z) \tag{1}$$

**III.6.7 Remark.** Formula (1) has $A$ as its only free variable. Of course, it is equivalent to a version that is prefixed with "$(\forall A)$". Now, this axiom is stated a bit too tersely (especially for our flavour of ZFC, which allows atoms) and needs some "parsing".

(a) (1) is provably equivalent to

$$\neg U(A) \rightarrow (\exists z)(\forall x)(\forall y)(x \in y \wedge y \in A \rightarrow x \in z) \tag{2}$$

Indeed, (2) is a tautological consequence of (1). Conversely, (1) follows from (2) and proof by cases, because we can also prove

$$U(A) \rightarrow (\exists z)(\forall x)(\forall y)(x \in y \wedge y \in A \rightarrow x \in z) \tag{3}$$

Let us do this. We have

$$U(A) \vdash_{\mathrm{ZFC}} \neg y \in A$$

Thus, by tautological implication,

$$U(A) \vdash_{\mathrm{ZFC}} x \in y \wedge y \in A \rightarrow x \in z$$

Now, generalization followed by an invocation of the substitution axiom gives

$$U(A) \vdash_{\mathrm{ZFC}} (\exists z)(\forall x)(\forall y)(x \in y \wedge y \in A \rightarrow x \in z)$$

from which the deduction theorem yields (3).

(b) (1) does not ask that $z$, whose existence it postulates, be a set (it could be an atom). However, we can show using (1) that

$$\vdash_{\mathrm{ZFC}} (\exists z)\Big(\neg U(z) \wedge (\forall x)(\forall y)(x \in y \wedge y \in A \rightarrow x \in z)\Big) \tag{4}$$

To see this, let $B$ be a $z$ that works (we are arguing by auxiliary constant) in (1). Thus we add (to ZFC) the assumption

$$(\forall x)(\forall y)(x \in y \wedge y \in A \rightarrow x \in B) \tag{5}$$

Hence

$$x \in y \wedge y \in A \rightarrow x \in B \tag{6}$$

We have two cases (proof by cases):

- Let (i.e., add) $\neg U(B)$. By (5) and tautological implication, we get

  $$\neg U(B) \wedge (\forall x)(\forall y)(x \in y \wedge y \in A \rightarrow x \in B)$$

  and then the substitution axiom yields (4).
- Let (i.e., add) $U(B)$. By III.1.3 and the assumption we obtain $\neg x \in B$; hence

  $$x \in B \rightarrow x \in \emptyset$$

  by tautological implication. (6) and tautological implication (followed by generalization) yield

  $$(\forall x)(\forall y)(x \in y \wedge y \in A \rightarrow x \in \emptyset)$$

  from which

  $$\neg U(\emptyset) \wedge (\forall x)(\forall y)(x \in y \wedge y \in A \rightarrow x \in \emptyset)$$

  Once again, the substitution axiom yields (4). □

**III.6.8 Proposition.** $\vdash_{\text{ZFC}}$ *$Coll_x\Big((\exists y \in A)x \in y\Big)$, where $A$ is a free variable.*

*Proof.* We use (4) of III.6.7(b). Add then a new constant $B$ and the assumption

$$\neg U(B) \wedge (\forall x)(\forall y)(x \in y \wedge y \in A \rightarrow x \in B)$$

Thus

$$\neg U(B) \tag{$i$}$$

and

$$x \in y \wedge y \in A \rightarrow x \in B \tag{$ii$}$$

We can now show that

$$(\exists y)(y \in A \wedge x \in y) \rightarrow x \in B \tag{$iii$}$$

which will rest the case by III.2.11 and $(i)$. Well, $(iii)$ follows from $(ii)$ by $\exists$-introduction. □

**III.6.9 Definition (The Formal Big $\bigcup$ and Little $\cup$).** For the record, we introduce into our theory a unary (1-ary) function symbol, "$\bigcup$", *formally*, by the defining axiom

$$\bigcup A = z \leftrightarrow \neg U(z) \wedge (\forall x)\big(x \in z \leftrightarrow (\exists y \in A)x \in y\big) \tag{1}$$

We also introduce a new binary (or 2-ary) function symbol, "$\cup$", by the defining axiom

$$x \cup y = \bigcup\{x, y\} \tag{2}$$

□

*Worth repeating*: If $\mathbb{A}$ is a set, then so is $\bigcup \mathbb{A}$. Indeed, the assumption translates to $Coll_x \mathscr{A}$; hence the class term $\mathbb{A}$ – that is, $\{x : \mathscr{A}\}$ – is (really, *names*) a formal term "$t$" of set theory. So is $\bigcup t$ by definition of terms, and III.6.9.

But is it an atom? Since $\vdash_{\mathrm{ZFC}} \neg U\Big(\bigcup x\Big)$ by the preceding definition, where $x$ is a free variable, $\vdash_{\mathrm{ZFC}} \neg U\Big(\bigcup t\Big)$ by substitution.

**III.6.10 Remark.** By III.6.8 the function $\bigcup$ "makes sense" for both set and atom variables. It is trivial to see from (1) above that

$$\vdash_{\mathrm{ZFC}} U(A) \to \bigcup A = \emptyset$$

It follows that the binary formal $\cup$ also makes sense for any arguments and that $\vdash_{\mathrm{ZFC}} U(A) \wedge U(B) \to A \cup B = \emptyset$. □

**III.6.11 Example.** What is $\bigcup\{a, b\}$? How does it relate to the *informal* definition (III.4.12, p. 141)? Let us calculate using III.6.3:

$$\begin{aligned}
\{x : (\exists y)(y \in \{a, b\} \wedge x \in y)\} &= \{x : (\exists y)((y = a \vee y = b) \wedge x \in y)\}\\
&= \{x : (\exists y)(y = a \wedge x \in y \vee y = b \wedge x \in y)\}\\
&= \{x : (\exists y)(y = a \wedge x \in y) \vee (\exists y)(y = b \wedge x \in y)\}\\
&= \{x : x \in a \vee x \in b\}\\
&= a \cup b
\end{aligned}$$

The second "=" from the bottom was by application of the "one-point rule" (I.6.2). Note that in "$a \cup b$" we are using the formal "$\cup$" to allow this term to be meaningful for both sets and atoms $a, b$.[†] □

**III.6.12 Informal Definition (Intersection of a Family).** *The intersection of a family* $\mathbb{F}$, in symbols $\bigcap \mathbb{F}$, stands for $\{x : (\forall y \in \mathbb{F})x \in y\}$.

If for every two $A$ and $B$ in a family $\mathbb{F}$ it is the case that $A \neq B \to A \cap B = \emptyset$, then we say that $\mathbb{F}$ consists of *pairwise disjoint sets* or is a pairwise disjoint family. □

[†] "$\bigcup\{a, b\}$" of III.6.3 is meaningful for both sets and atoms $a, b$. So is the formal "$\cup$" of III.6.9, unlike "$\mathbb{A} \cup \mathbb{B}$" of III.4.12, which is defined only for class arguments.

(1) *Operationally*, we certify things such as "$\mathbb{F}$ is a pairwise disjoint family" by proving in ZFC the defining property "$A \neq B \to A \cap B = \emptyset$ for all sets $A$ and $B$ in $\mathbb{F}$". Correspondingly, a statement such as "Let $\mathbb{F}$ be a pairwise disjoint family" is another way of saying "assume that $A \neq B \to A \cap B = \emptyset$ for all sets $A$ and $B$ in $\mathbb{F}$".

(2) We are not interested in the intersection of arbitrary classes (that may contain atoms, and hence *not* be families) in introducing the big-$\bigcap$ abbreviation. We will also make an exception to what we have practiced so far, and we will not introduce a formal counterpart for $\bigcap$.[†] It is sufficient that we have a formal little $\cap$.

Let $\mathbb{A} = \{x : \mathscr{A}[x]\}$. We have a number of variations in the notation for $\bigcap \mathbb{A}$: $\bigcap_{x \in \mathbb{A}} x$ or $\bigcap\{x : \mathscr{A}[x]\}$ or $\bigcap_{\mathscr{A}[x]} x$.

**III.6.13 Example.** Let $\mathbb{F} = \{\{1, 2\}, \{1, 3\}\}$ (this family is a set; working in the metatheory, apply pairing three times). Then $\bigcap \mathbb{F} = \{1\}$.

Let now $\mathbb{G}$ be any family, and $a \in \mathbb{G}$. Then $\bigcap \mathbb{G} \subseteq a$. Indeed, the translation of the claim (by III.6.12 and III.4.7) is

$$a \in \mathbb{G} \to (\forall y)(y \in \mathbb{G} \to x \in y) \to x \in a \tag{1}$$

We can prove (1) within pure logic: Assume $a \in \mathbb{G}$ and $(\forall y)(y \in \mathbb{G} \to x \in y)$. By specialization, $a \in \mathbb{G} \to x \in a$; hence (MP) $x \in a$. By the deduction theorem, (1) is now settled. What happens if $\mathbb{G} = \emptyset$? (See Exercise III.18.) □

**III.6.14 Proposition (Existence of Intersections).** *If the family $\mathbb{F}$ is nonempty, then $\bigcap \mathbb{F}$ is a set.*

*Proof.* By Example III.6.13 and separation (III.4.10). □

*Priorities of set operations*. "$-$" (that is, *difference* – as we will not use *complements*) and "$\cup$" have the same priority and associate right to left. "$\cap$" is stronger (associativity is irrelevant by Exercises III.19 and III.20). Thus $A - B \cup C = A - (B \cup C)$, while $A \cap B - C = (A \cap B) - C$, $A \cap B \cup C = (A \cap B) \cup C$. When in doubt, use brackets!

**III.6.15 Proposition (De Morgan's Laws for Classes).** *Let $\mathbb{A}, \mathbb{B}, \mathbb{C}$ be arbitrary classes. Then,*

(1) $\vdash \mathbb{C} - (\mathbb{A} \cup \mathbb{B}) = (\mathbb{C} - \mathbb{A}) \cap (\mathbb{C} - \mathbb{B})$ *and*
(2) $\vdash \mathbb{C} - (\mathbb{A} \cap \mathbb{B}) = (\mathbb{C} - \mathbb{A}) \cup (\mathbb{C} - \mathbb{B})$.

[†] We do not feel inclined to perform acrobatics just to get around the fact that $\bigcap \emptyset$ cannot be a formal term: it is not a set (see Example III.6.13 below).

*Proof.* We do (1) imitating the way people normally argue this type of thing, "at the element level". The proof uses pure logic and Definitions III.4.1, III.4.3, III.4.8, and III.4.12.

$\subseteq$: Let $x \in \mathbb{C} - (\mathbb{A} \cup \mathbb{B})$. Then

$$x \in \mathbb{C} \tag{$i$}$$

and

$$x \notin (\mathbb{A} \cup \mathbb{B}) \tag{$ii$}$$

By definition of $\cup$, $(ii)$ yields

$$x \notin \mathbb{A} \wedge x \notin \mathbb{B} \tag{$iii$}$$

Combine $(i)$ and $(iii)$ to get (by definition of difference)

$$x \in \mathbb{C} - \mathbb{A} \wedge x \in \mathbb{C} - \mathbb{B}$$

or (by definition of $\cap$)

$$x \in (\mathbb{C} - \mathbb{A}) \cap (\mathbb{C} - \mathbb{B})$$

Done, by the deduction theorem.

$\supseteq$: Let $x \in (\mathbb{C} - \mathbb{A}) \cap (\mathbb{C} - \mathbb{B})$. Then

$$x \in \mathbb{C} - \mathbb{A} \wedge x \in \mathbb{C} - \mathbb{B}$$

Hence

$$x \in \mathbb{C} \tag{$iv$}$$

and

$$x \notin \mathbb{A} \wedge x \notin \mathbb{B}$$

This last one says (by definition of $\cup$)

$$x \notin (\mathbb{A} \cup \mathbb{B})$$

which along with $(iv)$ gives

$$x \in \mathbb{C} - (\mathbb{A} \cup \mathbb{B})$$

Case (2) is left as Exercise III.26. □

**III.6.16 Example.** A better way, perhaps, is to use translations and reduce the issue to a tautology: (1) above translates to (III.4.1, III.4.3 and III.4.12)

$$\mathscr{C} \wedge \neg(\mathscr{A} \vee \mathscr{B}) \leftrightarrow (\mathscr{C} \wedge \neg\mathscr{A}) \wedge (\mathscr{C} \wedge \neg\mathscr{B})$$

Noting that (by propositional De Morgan's laws)

$$\models_{\textbf{Taut}} \mathscr{C} \wedge \neg(\mathscr{A} \vee \mathscr{B}) \leftrightarrow \mathscr{C} \wedge (\neg\mathscr{A} \wedge \neg\mathscr{B})$$

we are done. □

## III.7. Axiom of Foundation

**III.7.1 Example.** We have seen that the "absolute universe", $\mathbb{U}_M = \{x : x = x\}$, is a proper class.

The Russell paradox argument does not depend on what exactly $M$ is; therefore an alternate Russell class, $\{x \in \mathbb{U}_N : x \notin x\}$, exists in all alternate universes $\mathbb{U}_N$ (where $\emptyset \subseteq N \subseteq M$ – see III.4.20). Thus all universes $\mathbb{U}_N$ are also proper classes. □

**Informal Discussion (towards Foundation).** In preparation for the axiom of foundation, we next reexamine the "magic" of the statements $x \notin x$ and $x \in x$. Some people react to Russell's paradox by blaming it on an expectation that $x \in x$ might be true for some $x$. This is not the right attitude, regardless of what we think the answer to the question $x \in x$ is. After all, there is an alternative "theory of sets" where $x \in x$ *is* possible, and this theory *is* consistent if ZFC is – so, in particular, it does not suffer from Russell's paradox.[†]

What really *is* taking place in the Russell argument is a *diagonalization* – a technique introduced by Cantor to show that there are "more" real numbers than natural numbers – and this has nothing to do with whether $x \in x$ is, or is not, "really true".

We can visualize this diagonalization as follows. Arrange *all atoms and sets* into a matrix as in the figure below:

$$
\begin{array}{c|cccccccc}
 & a & b & c & D & B & A & X & \dots \\
\hline
a & i & i & i & i & i & i & i & \dots \\
b & i & i & i & i & i & i & i & \dots \\
c & i & i & i & i & i & i & i & \dots \\
D & i & i & i & i & i & i & i & \dots \\
B & i & i & i & i & i & i & i & \dots \\
A & i & i & i & i & i & i & i & \dots \\
X & i & i & i & i & i & i & i & \dots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}
$$

The $a, b, c, \dots$ that label the columns and rows are all the sets and atoms arranged in some fashion. We may call these labels the *heads* of the respective rows or columns that they label.

Each entry, $i$, can have the value 0 or 1 or the name of an atom (without loss of generality, we assume that no atom has as name 0 or 1). This value is

[†] See Barwise and Moss (1991) for an introduction to *hypersets*.

determined as follows:

$$\text{Entry at row } z \text{ and column } w = \begin{cases} 0 & \text{if } z \in w \\ 1 & \text{if } z \notin w \wedge \neg U(w) \\ w & \text{if } U(w) \quad \text{[N.B. This entails } z \notin w\text{]} \end{cases}$$

Here are a few examples: Say $a$ is an atom. Then all the $i$'s in column $a$ have value $a$. Let $b = \{b, D\}$.[†] Then column $b$ has 1 everywhere except on rows $b$ and $D$, where it has 0. Conversely, the head of a column sequence of 0, 1, and atom values is determined by the sequence.[‡] For example, the sequence of 1 everywhere determines ∅; the sequence

$$110\underbrace{1\ldots}_{\text{all } 1}$$

i.e., the one that has 1 everywhere except at (row) position $c$, where it has a 0, determines the set $\{c\}$.

Let us now define informally a sequence, and therefore a *class* that we will call $\widehat{R}$, by going along the *main diagonal* (that is, along the matrix entries $(a, a)$, $(b, b)$, $(c, c)$, ...) "reversing" all the $i$-values (specifically, nonzero to 0 and 0 to 1). That is,

$$\text{the sequence for } \widehat{R} \text{ has a } \begin{cases} 0 \text{ at position } x \text{ if entry}(x, x) \text{ is } \textit{not} \text{ a } 0 \\ 1 \text{ at position } x \text{ if entry}(x, x) \textit{ is} \text{ a } 0 \end{cases} \tag{1}$$

It follows that the sequence for $\widehat{R}$ differs from the sequence for *any* $x$ at position $x$.

Thus, $\widehat{R}$ *cannot* occur anywhere in the matrix (as a column) – for if it occurred as column $x$, it then would be "schizophrenic" at matrix entry $(x, x)$ – so it is not a set (recall, the matrix represents *all* sets and atoms as columns).

What is the connection with Russell's paradox? Well, in (1) we are saying that $x \in \widehat{R}$ iff $x \notin x$; hence $\widehat{R} = R$, the Russell class! The above diagonalization can be readily adapted to "construct" a set that is not in a given set $b$. All we have to do is to think of the matrix as "listing", or representing, just all the atoms and sets *in b* rather than in $\mathbb{U}_M$ (see Exercise III.6).

[†] In view of what we said in the preceding footnote regarding hypersets, we allow *just for the sake of this discussion* the generality where $b \in b$ *is* possible.

[‡] Do not expect *all* sequences to appear as columns. For example the sequence whose members are all 0 denotes $\mathbb{U}_M$, but our matrix heads are only sets or atoms.

We have *chosen* to describe (by ZFC) a standard model where, among its properties, we have that $x \in x$ is always false, by Principle 1.[†] Similarly, $a \in b \in a$ and, more generally, $a \in b \in \cdots \in a$ are absurd in our model, for the leftmost $a$ should be available before the rightmost $a$ for such a chain of memberships to be valid (Principle 1).

Note that if, say, $a \in b \in a$ were possible, then we would get the "infinite" chain

$$\cdots a \in b \in a \in b \in a \in b \in a \tag{1}$$

i.e., $a$ would be "bottomless", like an infinite regression of a "box in a box in a box in a box . . . ". Sets that are *not* bottomless are called *well-founded*.

A bit more can be said of the standard model. It is not only "repeating" chains such as (1) that are not possible, but likewise non-repeating infinite "descending" chains such as

$$\cdots a_n \in a_{n-1} \in \cdots \in a_2 \in a_1 \in a_0 \tag{2}$$

There are no bottomless sets, period.

Towards formulating an appropriate axiom of ZFC that says "bottomless sets do not exist", let $\mathbb{A}$ be any nonempty class. Assume that it contains no atoms. Now, there must be a set (maybe more than one) in $\mathbb{A}$ that was constructed *no later than any other set in* $\mathbb{A}$ (for example, if # and | name atoms, and if $\{\#\} \in \mathbb{A}$ and $\{|\} \in \mathbb{A}$, then $\{\#\}$ and $\{|\}$ are two among those sets in $\mathbb{A}$ that are constructed the earliest possible).

Let now, in general, $y$ be such an earliest-constructed set in $\mathbb{A}$, and let $x \in y$. It follows that $x \notin \mathbb{A}$ (for $x$ is an atom – hence not in $\mathbb{A}$ – or is a set built *before* $y$). The existence of sets like $y$ in $\mathbb{A}$ captures *foundation*. Thus, taking $\mathbb{A}$ to contain precisely the members of (2), we see that (2) is absurd. ☡

**III.7.2 Axiom (Foundation Schema).** *Class form:*

$$\mathbb{A} \neq \emptyset \to (\exists y \in \mathbb{A})(\neg(\exists x \in y)x \in \mathbb{A})$$

*or, applying De Morgan's laws,*

$$\mathbb{A} \neq \emptyset \to (\exists y \in \mathbb{A})(\forall x \in y)x \notin \mathbb{A}$$

*The axiom expressed in the formal language is the schema*

$$(\exists y)\mathscr{A}[y] \to (\exists y)(\mathscr{A}[y] \wedge \neg(\exists x \in y)\mathscr{A}[x])$$

[†] Note that in such a state of affairs all entries $(x, x)$ are nonzero; thus $\widehat{R}$ is the sequence composed entirely of 0, representing $\mathbb{U}_M$. This is as it is expected, since now $R = \mathbb{U}_M$.

**III.7.3 Remark.**

(1) The foundation axiom (schema) is also called the *regularity axiom*.

(2) The schema version of foundation is due to Skolem (1923). It readily implies – using $\mathscr{A} \equiv y \in A$ – *and* is implied[†] by the single-axiom (non-schema) set version where $A$ is a free variable other than $y$:

$$(\exists y) y \in A \rightarrow (\exists y)\big(y \in A \wedge \neg(\exists x \in y) x \in A\big)$$

or

$$\neg U(A) \rightarrow A \neq \emptyset \rightarrow (\exists y \in A)(\neg(\exists x \in y) x \in A)$$

(3) The discussion that motivated III.7.2 was in terms of a class $\mathbb{A}$ that contained no atoms. No such restriction is stated in III.7.2, for trivially, if $\mathbb{A}$ does contain atoms, any such atom will do for $y$. If it is known that $\mathbb{A}$ is a *family* of sets (i.e., that it contains no atoms), then foundation simplifies to

$$\mathbb{A} \neq \emptyset \rightarrow (\exists y \in \mathbb{A}) y \cap \mathbb{A} = \emptyset$$

(4) If for a minute we write $<$ for $\in$, then III.7.2 (formal language version) reads exactly as the least number principle on $\mathbb{N}$. Of course, $\in$ is not an order on all sets; however, if its scope is restricted on appropriate sets, then it becomes an order, and III.7.2 makes it a *well-ordering*. More on this in Chapter VI. □

**III.7.4 Example.** Let us derive once again the falsehood of $a \in a$ and $a \in b \in a$, this time formally, using the axiom (schema) of foundation.

Given $a$ and $b$ (sets or atoms), the sets $S = \{a\}$ and $T = \{a, b\}$ exist,[‡] as we saw earlier. Since $S \neq \emptyset$, there is a $y \in S$ such that $x \in y$ is false for all $x \in S$ (III.7.2). The only candidate for either $y$ or $x$ is $a$. Thus, $a \in a$ is false.

O.K., let us repeat the above in a (formal) manner so that we will not be accused of arguing semantically (saying things like “false” – colloquial for “refutable” – and the like):

$$\vdash_{\mathrm{ZFC}} \neg U(\{a\}) \rightarrow \{a\} \neq \emptyset \rightarrow (\exists y \in \{a\})(\neg(\exists x \in y) x \in \{a\})$$

by III.7.3(2) and III.5.5. Since $\vdash_{\mathrm{ZFC}} \neg U(\{a\})$ and $\vdash_{\mathrm{ZFC}} \{a\} \neq \emptyset$, modus ponens yields

$$\vdash_{\mathrm{ZFC}} (\exists y \in \{a\})(\neg(\exists x \in y) x \in \{a\}) \tag{1}$$

[†] Not so readily. We will get to this later.

[‡] “The set $\{a\}$ exists” is another way of saying that “$\{a\}$ is a set” or that “the term $\{a\}$ can be formally introduced”.

Let $B$ be a new constant, and add the assumption

$$B \in \{a\} \wedge \neg(\exists x)(x \in B \wedge x \in \{a\}) \tag{2}$$

or, as we say when we act like Platonists, "let $B$ be an object such as (1) tells us exists". From (2) we derive $B \in \{a\}$ hence, by III.5.5,

$$B = a \tag{3}$$

and

$$\neg(\exists x)(x \in B \wedge x \in \{a\})$$

which in view of (3) and III.5.5 yields

$$\neg(\exists x)(x \in a \wedge x = a)$$

i.e., ("one point rule", I.6.2, p. 71)

$$\neg a \in a$$

We have just refuted $a \in a$ ($a$ a free variable).

For $T$ we only offer the informal (Platonist's) argument: There is a $y \in T$ such that $x \in y$ is false for all $x \in T$.

Case where $y = a$: Then we cannot have $b \in a$.
Case where $y = b$: Then we cannot have $a \in b$.

So we cannot have both $a \in b$ and $b \in a$ (i.e., $a \in b \in a$). □

## III.8. Axiom of Collection

In older approaches to set theory, when the formation-by-stages doctrine was not available, how did mathematicians recover from paradoxes? "Sets"[†] like $R$ and $\mathbb{U}_M$ were known to be "paradoxical", and this was attributed to their enormous size. In turn, this uncontrollable size resulted into some of these "sets" becoming members of themselves, a situation that was (incorrectly) considered in itself as paradoxical and a source of serious logical ills – such was the impact of Russell's paradox and the central presence of the "self-referential statement"[‡] $x \in x$ in its derivation. For example, the "self-contradictory" (as they called it) "set of all sets", $\mathbb{V}_M$, certainly satisfied, according to the analysis at that time, $\mathbb{V}_M \in \mathbb{V}_M$.

[†] We use the term "set" in quotes because at the time in the development of set theory that this commentary refers there was no technical distinction between sets and proper classes. Rather, there was a distinction between "sets" and "self-contradictory" sets; they were all sets, but some were troublemakers and were avoided.

[‡] If $x$ could talk, it would say "I am a member of myself".

That this was considered to be a "problem" can be seen, for example, in Kamke (1950, p. 136) where he states that all "sets", such as (Russell's) $R$ and $\mathbb{V}_M$, "that contain themselves as elements are 'self-contradictory' concepts as a matter of course, and are therefore inadmissible". He adds that no sets that contain themselves are known that reasonable people would "regard as meaningful sets".[†]

So the "set of all sets" was to be avoided at all costs.[‡] But how do you define "large"? In the absence of an exact definition, at the one extreme you may be out on a witch hunt, and at the other extreme you may be the victim of error (see III.8.1). Are all large "sets" members of themselves? (Again, see III.8.1.)

Of course, all these worries were for the mathematician who worked on the foundations of mathematics. The analyst, the number theorist, and the topologist were not worried by such issues, for they worked in "small universes", or "reference sets". That is, $\mathbb{R}$ (reals) or $\mathbb{C}$ (complex numbers) or $\mathbb{Z}$ would be the reference sets of the analyst and number theorist: all the atoms they needed were members of these reference sets, and any sets they needed were subsets of the reference sets. The topologist too would be satisfied to start with some "small" space (set), $X$, his reference, and then study subsets of $X$, looking for "open" sets, "closed" sets, "connected" sets, etc.

In elementary expositions of set theory, even contemporary ones, the reference set approach is sometimes misrepresented as a logical necessity for the avoidance of paradoxes.

Let us conclude this discussion by proposing a new *informal (metamathematical) principle*, which invokes "largeness" in a relative sense (Cantor's work implicitly used this principle, which was first articulated by Russell). This principle, on one hand, yields – by a different route – the axiom of separation; on the other hand it yields the important axiom of *replacement*.

**Principle 3 (The Size Limitation Doctrine).** A class is a set if it is *not* "larger" than some known set. Correspondingly, it is not a set if it is as large as a *proper* class, for, otherwise this proper class would also be a set.

"Largeness" we will leave undefined, but this drawback is not serious, for we will apply the principle (carefully, and only twice) just to "derive" two axioms.

[†] The reader is reminded of the nowadays acknowledged existence of such (hyper)sets (Barwise and Moss (1991)) – not, however in ZFC.

[‡] Indeed, mathematicians were suspicious of even the phrase "all sets" in something as innocent as "…let us divide all possible sets into [equivalence] classes…" (N.B. Just *let us divide*, not attempt to *collect* into a "set".) See Wilder (1963, p. 100) for further discussion, where he speculates whether the "concept" of "all sets" might be as "self-contradictory" as the concept of "the set of all sets".

After this has been accomplished, we will forget Principles 0–3 and always defer to the axioms.

**III.8.1 Example.** Let $B$ be a set and let $\mathbb{A} \subseteq B$. Then certainly $\mathbb{A}$ is not larger than $B$, so $\mathbb{A}$ is a set by Principle 3. Thus separation (see the class form of the schema, III.4.10) follows from the doctrine of size limitation as much as it follows from that of set formation by stages.

Next, let $\mathbb{U}'$ be the class of all *singletons*. Is this class "large" (hence proper), or is it "small" (hence a set)? This example appears in Wilder (1963, p. 100) (see in particular the closing remarks prior to his 4.1.2), where the argument implies that this "set" is *not* "self-contradictory" (what we now call a "proper class"), for, after all, it is far from containing "all sets". In fact, in 4.1.2 (*loc. cit.*) the "cardinal number 1" is identified with the "set" of all singletons ($\mathbb{U}'$) without any adverse comment.

Well, it turns out that $\mathbb{U}'$ *is* a proper class, for it has the same size as $\mathbb{U}_M$, as we can readily see from the fact that each $x \in \mathbb{U}_M$ corresponds to a unique $\{x\} \in \mathbb{U}'$ and vice versa. Thus, as a "set", $\mathbb{U}'$ would be every bit as "self-contradictory" as $\mathbb{U}_M$. Incidentally, we must wonder to what extent the fact that, as a "set", $\mathbb{U}'$ clearly satisfied $\mathbb{U}' \notin \mathbb{U}'$ made it more acceptable than $\mathbb{U}_M$ back then. □

Now consider a set $A$. Let us next "replace" every element $x \in A$ by some other object $x'$ (set or urelement).[†]

Evidently, the resulting class (let us call it $\mathbb{A}$) is not larger than the original (and could very well be smaller, for we might have replaced several $x \in A$ by the same object); hence, by Principle 3, $\mathbb{A}$ is a *set*. This is the principle of (it goes under several names) *replacement* or *substitution* or *collection*, and it is very important in ZFC.

*We prefer not to use the name "substitution" for this nonlogical axiom, for that would clash with our use of the name for the logical axiom*

$$\mathscr{A}[x \leftarrow t] \to (\exists x)\mathscr{A}$$

*We will adhere to the name "collection".*

Below we state it as an axiom in the formal language. In the next section, once the notions of *relation* and *function* have been formalized, we will give a very simple version of the axiom.

[†] We use "replace" in the weak sense, where it is possible that for one or more $x \in A$ the replacing object is the same as the replaced object.

**III.8.2 Axiom (Schema of Collection or Replacement).** *For any formula* $\mathscr{P}[x, y]$,

$$(\forall x \in A)(\exists y)\mathscr{P}[x, y] \to (\exists z)(\forall x \in A)(\exists y \in z)\mathscr{P}[x, y] \qquad (1)$$

*where* $A$ *is a free variable.*

**III.8.3 Remark.** (I) In any specific instance of the axiom (schema) of collection the formula $\mathscr{P}[x, y]$ is the "agent" that effects the replacements: The hypothesis ensures that for each $x \in A$, $\mathscr{P}$ suggests a $y$ (maybe it has more than one suggestion) – depending on $x$ – as a possible replacement.

The conclusion says that there is a *set*,[†] $z$, which contains, *instead of each x that was originally in* $A$, one (or more) replacement(s), $y$, among the possibly many that were suggested by $\mathscr{P}$. (All the suggestions were made to the left of "→".)

There is a small difficulty here: In the formal statement adopted in III.8.2 – where we have allowed *more than one possible candidate* $y$ to replace each $x$ – we run at once into a size *and* a "definability" problem: Obviously, if we are going to argue that the size of $z$ is small (and hence $z$ is a set) we have to be able to

(a) either choose a unique replacement $y$ for each $x \in A$ (and $\mathscr{P}[x, y]$ cannot help us here; *we* have to do the choosing), or
(b) choose a "very small number" of replacements $y$ for each $x \in A$ – i.e., cut down the size of the class of replacement values for each $x$ – so that the size of $z$ *is not substantially different* from that of $A$.[‡]

If we were to take approach (a), then we would need a mechanism to effect infinitely many choices, *one out of each class* $\mathbb{A}_x = \{y : \mathscr{P}[x, y]\}$, thus in effect turning the hypothesis into $(\forall x \in A)(\exists! y)\mathscr{Q}[x, y]$ (where $\mathscr{Q}[x, y] \to \mathscr{P}[x, y]$, for all $x \in A$) so that we could benefit from the size argument preceding III.8.2. However, this would require (a strong form of) the axiom of choice, the axiom that says, in effect, "don't worry if you cannot come up with a *well-defined* method to form a set consisting of one element out of each set in a (set) family of sets; such a set exists anyhow".

[†] Well, not exactly. It says that a *formal object* exists, but this object could well be an atom. Since we will prove (III.8.4) an equivalent statement to (1), which explicitly asks that $z$ *be* a set, we can pretend in this discussion that (1) already asks that $z$ be a set, although it does so between the lines.

[‡] Clearly, it is not "safe" to collect into $z$ *all* possible $y$ that $\mathscr{P}[x, y]$ yields for each $x$. For example, if $\mathscr{P}[x, y] \equiv x \subseteq y$ and $A = \{\emptyset\}$, then allowing *all* the $y$ that $\mathscr{P}$ yields for $x \in A$ we would end up with $z = \mathbb{U}_M$, not a set.

We can do better than that (avoiding the axiom of choice, which we have not formally introduced yet) if we allow ourselves to put in $z$ possibly *more than one* $y$ that satisfy $\mathscr{P}[x, y]$ for a given $x \in A$, that is, approach (b). We do this as follows: To show (informally) that a set $z$ as claimed by the formal axiom exists, and that therefore the axiom is "really true", let us consider, for each $x \in A$, *all* the $y$ such that $\mathscr{P}[x, y]$ is true which *are built at the earliest possible stage*. There is just one such stage for each $x$, call it $\Sigma_x$. Now the class of all such $y$, call it $Y_x$, is a set, for all its elements are available at stage $\Sigma_x$, and there certainly is a stage after $\Sigma_x$ (at such a stage, $Y_x$ is formed as a set).

Thus, for each $x \in A$ we ended up with a *unique* set $Y_x$. Using the informal analysis prior to the axiom, there is a *set* $B$ that contains exactly all the $Y_x$. It is clear now that we can "well-define" $z$: $z = \bigcup B$ will do, and is a set by the union axiom.

(II) The hypothesis part of the axiom is usually stated in stronger terms, viz., $(\forall x \in A)(\exists! y)\mathscr{P}[x, y]$,[†] and in that format it usually goes under the name *replacement* axiom. The present form (mostly known as the *collection* axiom, e.g., Barwise (1975)) is clearly preferable, for to apply it we have to work less hard to recognize that the hypothesis holds. All the various formulations of collection/replacement are equivalent in ZF (even without the "C"). Some other forms besides the ones stated so far are the following, where we are using set term notation in the interest of readability:

(1) Bourbaki (1966b):

$$(\forall x)(\exists z)(\forall y)(\mathscr{P}[x, y] \rightarrow y \in z) \rightarrow (\forall A)Coll_y(\exists x \in A)\mathscr{P}[x, y]$$

or in more suggestive notation

$$(\forall x)(\exists z)\{y : \mathscr{P}[x, y]\} \subseteq z \rightarrow (\forall A)Coll_y(\exists x \in A)\mathscr{P}[x, y]$$

(2) Shoenfield (1967):

$$(\forall x)(\exists z)(\forall y)(\mathscr{P}[x, y] \leftrightarrow y \in z) \rightarrow (\forall A)Coll_y(\exists x \in A)\mathscr{P}[x, y]$$

or in more suggestive notation[‡]

$$(\forall x)(\exists z)\{y : \mathscr{P}[x, y]\} = z \rightarrow (\forall A)Coll_y(\exists x \in A)\mathscr{P}[x, y]$$

[†] Recall that $(\exists! x)\mathscr{R}$ says that there is a *unique* $x$ satisfying $\mathscr{R}$. That is, $(\exists x)(R[x] \wedge (\forall y)(y \neq x \rightarrow \neg R[y]))$.

[‡] The "suggestive" notation in (1) above is 100% faithful to the formal version, since, by III.3.6, $(\forall y)(\mathscr{P}[x, y] \rightarrow y \in z)$ is provably equivalent to $\{y : \mathscr{P}[x, y]\} \subseteq z$ (see also III.1.5, p. 116). Not so for the suggestive rendering of (2) *in the presence of atoms*. For example, on the assumption $U(z)$, $(\forall x)(\neg x = x \leftrightarrow x \in z)$ is not equivalent to $\{x : \neg x = x\} = z$. Well, on one hand

(3) Levy (1979):

$$(\forall x)(\forall y)(\forall y')(\mathscr{P}[x, y] \wedge \mathscr{P}[x, y'] \to y = y') \\ \to (\forall A)Coll_y(\exists x \in A)\mathscr{P}[x, y]$$

We can readily prove (III.8.12 below) that collection implies all these alternative forms. While the converse is true, it will have to wait until we can formalize "stages" and thus formalize the argument we have used in (I) above to show that collection is "really true".

(III) We have restricted the way in which sets become available, namely, requiring that they be built in stages, or that they be not much larger than their "parents" (i.e., the sets that we have used to build them). In the process, we developed (most of, but not all yet) the ZFC axioms, as they flow from these doctrines, with the apparent result of managing to escape from the paradoxes and antinomies of the past.

Thus, despite the lack of a (meta)proof of the consistency for ZFC, we are doing well so far. But is this apparent success at no cost? Have we got "enough sets" in this restricted axiomatic set theory to *mirror* what we normally do in everyday mathematics? Put another way, do we have *enough stages of set construction* in order to build sets that are as complicated as the various branches of mathematics require them to be?

Of course, this is not a quantitatively precise question, and it will not get a quantitatively precise answer. However, the answer will hopefully satisfy us that we are doing well on this count too.

Imagine two mathematicians who are playing the following game: They have a large and complicated set, $A$, to start with. They take turns, each taking an $x \in A$, "making his move", and then discarding $x$. A "move" consists of proposing the wildest, most complicated set of one's experience that one can think of on the spur of the moment: $S_x$. Of course, at each move each player is doing his best to utterly demolish the morale of his opponent and also to better his own effort at his previous move.

At the end of the game, we have a class of all the $S_x$, which is a set by collection. Now, the stage at which this class was built as a set is beyond the wildest imagination of our two friends – otherwise one of them would have proposed some set built at that stage during the game.

Shoenfield (1967) does not employ atoms, so that our rendering of (2) captures exactly what this form of collection "says" in *loc. cit.* On the other, this is a moot point, for we prove (III.8.12) that the formal version (2) – *even in the presence of atoms* – implies version (3) *without* adding the qualifier "$\neg U(z) \wedge$" before "$(\forall y)$". In turn, we find out later that form (3) implies collection. In short, versions (1) and (2), *exactly as stated*, are equivalent to our collection.

Put another way, we cannot "stretch" an "infinite" set $A$ into a proper class by the device of replacing each of $A$'s elements with horrendously complicated sets – i.e., sets that are built extremely late in the stage hierarchy – in an effort to run out of stages. Starting with $A \in \mathbb{U}_M$, no matter how far we stretch it, we still end up inside $\mathbb{U}_M$. Therefore, we do have a lot of stages. Equivalently, our "universe" is "very large".

There is an important observation to be made here: The reason that we have used the size doctrine to justify collection/replacement is, intuitively, precisely the result of the game above. We felt that we could not apply Principle 2 (p. 102) reliably, or convincingly, towards arguing that "we could imagine" that a stage existed after all the stages for the construction of all the sets $S_x$ (our two colleagues could not imagine either).

The reader is referred to Manin (1977, p. 46), where he states that – in the context of the doctrine of set formation by stages – the justification of the collection axiom goes beyond the "usual *intuitively obvious*". □

**III.8.4 Remark (a More Verbose Collection).** We "parse" here (just as we did for the axiom of union in III.6.7) the collection statement, extracting in the process more information from the axiom than it seems to be stating.

(I) First off, we never said that $A$ has to be a set. Indeed, III.8.2 is equivalent to

$$\neg U(A) \to (\forall x \in A)(\exists y)\mathscr{P}[x, y] \to (\exists z)(\forall x \in A)(\exists y \in z)\mathscr{P}[x, y] \tag{2}$$

This is because (2) is a tautological consequence of (1) in III.8.2 on the one hand. On the other hand, proof by cases with the help of

$$\vdash_{\mathrm{ZFC}} U(A) \to (\forall x \in A)(\exists y)\mathscr{P}[x, y] \to (\exists z)(\forall x \in A)(\exists y \in z)\mathscr{P}[x, y] \tag{3}$$

combines with (2) to derive collection as originally stated. Why is (3) valid? We can prove the simpler

$$\vdash_{\mathrm{ZFC}} U(A) \to (\exists z)(\forall x \in A)(\exists y \in z)\mathscr{P}[x, y] \tag{4}$$

from which (3) follows tautologically: Well, assume $U(A)$. Then $\neg x \in A$ by III.1.3, from which

$$x \in A \to (\exists y \in z)\mathscr{P}[x, y]$$

by tautological implication. Generalization followed by an invocation of the substitution axiom (and modus ponens) finally yields

$$(\exists z)(\forall x \in A)(\exists y \in z)\mathscr{P}[x, y]$$

Thus, we do not need to worry whether or not the variable $A$ appearing in the collection axiom is a set.

(II) Next we prove that

$$(\forall x \in A)(\exists y)\mathscr{P}[x, y] \to (\exists z)\Big(\neg U(z) \wedge (\forall x \in A)(\exists y \in z)\mathscr{P}[x, y]\Big) \tag{5}$$

is equivalent to collection. It is trivial that (5) implies collection, so we concentrate in the direction where collection implies (5). We use the deduction theorem, assuming

$$(\forall x \in A)(\exists y)\mathscr{P}[x, y] \tag{6}$$

under three cases: $U(A)$; $\neg U(A)$ and $A \neq \emptyset$; $A = \emptyset$.

Of course, $\vdash U(A) \vee \neg U(A) \wedge (A = \emptyset \vee A \neq \emptyset)$.

- $A = \emptyset$ or $U(A)$. This yields $\neg x \in A$ ($x$ free – see III.3.5 in case $A = \emptyset$); thus

  $$x \in A \to (\exists y \in \emptyset)\mathscr{P}[x, y]$$

  by tautological implication. Another tautological implication and $\vdash_{\text{ZFC}} \neg U(\emptyset)$ yield

  $$\neg U(\emptyset) \wedge (x \in A \to (\exists y \in \emptyset)\mathscr{P}[x, y])$$

  Following this up with generalization (and distribution of $\forall$ over $\wedge$, noting the absence of free $x$ in $\neg U(\emptyset)$), we have

  $$\neg U(\emptyset) \wedge (\forall x \in A)(\exists y \in \emptyset)\mathscr{P}[x, y]$$

  Thus, by the substitution axiom

  $$(\exists z)\Big(\neg U(z) \wedge (\forall x \in A)(\exists y \in z)\mathscr{P}[x, y]\Big)$$

  *Note*. Neither collection nor (6) was needed in this case.

- $\neg U(A)$ and $A \neq \emptyset$. The assumption amounts to $(\exists y) y \in A$. We argue by auxiliary constant. Let $B$ be a new constant, and assume

  $$B \in A \tag{7}$$

  By (6) collection yields

  $$(\exists z)(\forall x \in A)(\exists y \in z)\mathscr{P}[x, y] \tag{8}$$

Add yet another new constant, $C$, and assume

$$(\forall x \in A)(\exists y \in C)\mathscr{P}[x, y] \tag{9}$$

Specialization of (9) using (7) and modus ponens yields

$$(\exists y \in C)\mathscr{P}[B, y]$$

Hence

$$(\exists y)y \in C$$

by $\exists$-monotonicity (I.4.23). Thus (by III.1.3)

$$\neg U(C) \tag{10}$$

(9) and (10) tautologically imply $\neg U(C) \wedge (\forall x \in A)(\exists y \in C)\mathscr{P}[x, y]$, which by substitution axiom gives

$$(\exists z)\Big(\neg U(z) \wedge (\forall x \in A)(\exists y \in z)\mathscr{P}[x, y]\Big)$$

(III) Finally, collection is equivalent to

$$\begin{aligned} \neg U(A) \rightarrow (\forall x \in A)(\exists y)\mathscr{P}[x, y] \\ \rightarrow (\exists z)\Big(\neg U(z) \wedge (\forall x \in A)(\exists y \in z)\mathscr{P}[x, y]\Big) \end{aligned} \tag{11}$$

for (11) trivially implies (2), while (2) implies (11) using the two cases $A = \emptyset$ and $A \neq \emptyset$ exactly as we did above. □

**III.8.5 Remark (A Note on Nonlogical Schemata and Defined Symbols).** By I.6.1 and I.6.3, the addition of defined predicate, function, and constant symbols to any language/theory results in a conservative extension of the theory, that is, any theorem of the new theory over the original language is also provable in the original theory. Moreover, any formula $\mathscr{A}$ of the extended language can be naturally transformed back into a formula $\mathscr{A}^*$ of the old language (by eliminating all the defined symbols), so that

$$\mathscr{A} \leftrightarrow \mathscr{A}^* \tag{1}$$

is provable *in the extended theory*.

There is one potential worry about the presence of *nonlogical schemata* – such as the separation, foundation, and collection axiom schemata – that we need to address: Nonlogical axioms and schemata are specific to a theory and its *basic language*, i.e., the language prior to any extensions by definitions. For example, the collection schema III.8.2 (p. 163) is a "generator" that yields a specific nonlogical axiom (an *instance* of the schema) for each specific formula, *over the basic language* $L_{\text{Set}}$, that we care to substitute into the metavariable $\mathscr{P}$. There is no *a priori* promise that the schema "works" whenever we replace the syntactic variable $\mathscr{P}[x, y]$ by a specific formula, say "$\mathscr{B}$", over a language that is an extension of $L_{\text{Set}}$ by definitions.

For example,[†] do we have the right to expect the provability of

$$(\forall x \in A)(\exists y)y = t[x] \to (\exists z)(\forall x \in A)(\exists y \in z)y = t[x]$$

*in the extended theory*, if the term $t$ contains defined function or constant symbols?

Indeed we do, for let us look, in general, at an instance of collection obtained in the extended language by substituting the specific formula $\mathscr{B}$ – that *may* contain defined symbols – into the syntactic variable $\mathscr{P}$:

$$(\forall x \in A)(\exists y)\mathscr{B}[x, y] \to (\exists z)(\forall x \in A)(\exists y \in z)\mathscr{B}[x, y] \tag{2}$$

We argue that (2) is provable in the extended theory; thus *the axiom schema is legitimately usable in any extension by definitions of set theory over* $L_{\text{Set}}$.

Following the technique of symbol elimination given in Section I.6 (cf. I.6.4, p. 73) – eliminating symbols at the atomic formula level – we obtain the following version of (2), *in the basic language* $L_{\text{Set}}$. This translated version has exactly the same form as (2) (i.e., of collection), namely

$$(\forall x \in A)(\exists y)\mathscr{B}^*[x, y] \to (\exists z)(\forall x \in A)(\exists y \in z)\mathscr{B}^*[x, y]$$

Thus – being a collection schema instance over the basic language – it *is* an axiom of set theory, and hence also of its extension (by definitions).

Now, by (1), the equivalence theorem yields the following theorem of the extended theory:

$$\begin{aligned} &\Big((\forall x \in A)(\exists y)\mathscr{B}[x, y] \to (\exists z)(\forall x \in A)(\exists y \in z)\mathscr{B}[x, y]\Big)\\ \leftrightarrow\\ &\Big((\forall x \in A)(\exists y)\mathscr{B}^*[x, y] \to (\exists z)(\forall x \in A)(\exists y \in z)\mathscr{B}^*[x, y]\Big)\end{aligned}$$

Hence (2) is a theorem of the extended theory as claimed.

The exact same can be said of the other two schemata (foundation, separation).[‡] □

[†] This scenario materializes below, in III.8.9.

[‡] One can rethink the axioms, for example adopting Bourbaki's collection instead of our III.8.2, so that the separation schema becomes redundant. We have already promised to prove in due course that foundation need not be a schema. However, it turns out that we cannot eliminate all schemata. It is impossible to have a finite set of axioms equivalent to the ZFC axioms. We prove this result in Chapter VII.

**III.8.6 Example (Informal).** We often want to collect into a set objects that are more complicated than [“values of”] variables, subject to a *condition* being true. For example, we often write things such as

(1) $\{n^2 : n \in \mathbb{N}\}$,
(2) $\{x + y : x \in \mathbb{R} \wedge y \in \mathbb{R} \wedge x^2 + y^2 = 1\}$,
(3) $\{(x, y) : x \in \mathbb{R} \wedge y = 2\}$, where “$(x, y)$” is the “ordered pair” (more on which shortly) of the Cartesian coordinates of a point on the plane,
(4) $\{(x, y) : x \in \mathbb{R}\}$.

We are clear on what we mean by these shorthand notations. First off, for example, notation (1) cannot be possibly obtained in any manner by substitution from something like $\{x : \ldots x \ldots\}$, since the “$x$” in a set term $\{x : \mathscr{A}\}$ is bound. What we do mean is that we want to collect all objects that have the form “$n^2$” for some $n$ in $\mathbb{N}$. That is, notation (1) is shorthand (*abbreviation* or *argot*) for

$$\{x : (\exists n)(x = n^2 \wedge n \in \mathbb{N})\}$$

Similarly with (2)–(4). (4) is interesting in that $y$ is a free variable, or a *parameter* as we often say. We get different sets for different “values” of $y$. The shorthand (4) stands for the term $\{z : (\exists x)(z = (x, y) \wedge x \in \mathbb{R})\}$.

The notation reviewed here is sufficiently important to motivate the definition below. □

**III.8.7 Informal Definition (Collecting Formal Terms).** The symbol

$$\{t[\vec{w}_m] : \mathscr{A}[\vec{x}_n]\}$$

where $t[\vec{w}_m]$ is a *formal* term (cf. discussion following III.2.5), is *an abbreviation* of the class term

$$\Big\{y : (\exists x_1)(\exists x_2) \cdots (\exists x_n)\big(y = t[\vec{w}_m] \wedge \mathscr{A}[\vec{x}_n]\big)\Big\} \tag{1}$$

The variables $\vec{x}_n$ explicitly quantified in (1) above are precisely the ones we list in “$[\vec{x}_n]$” of $\mathscr{A}$. We may call them “linking” variables (linking the term $t$ with the “condition” $\mathscr{A}$) or “active” variables (Levy (1979)). All the remaining variables other than $y$ are free (parameters).

The notation does not always unambiguously indicate the active variables. In such cases the context, including surrounding text, will remove any ambiguity. □

**III.8.8 Example.** What does

$$\bigcup\{t[x] : \mathscr{A}[x]\}$$

abbreviate? In the first instance, it abbreviates the expression

$$\bigcup\{y : (\exists x)(y = t[x] \wedge \mathscr{A}[x])\}$$

The latter abbreviates (cf. III.6.3)

$$\Big\{z : (\exists y)\big((\exists x)(y = t[x] \wedge \mathscr{A}[x]) \wedge z \in y\big)\Big\} \tag{2}$$

Let us simplify (2):

$$\begin{aligned}
& (\exists y)\big((\exists x)(y = t[x] \wedge \mathscr{A}[x]) \wedge z \in y\big) \\
\leftrightarrow\ & \Big\langle z \in y \text{ has no free } x \Big\rangle \\
& (\exists y)(\exists x)(y = t[x] \wedge \mathscr{A}[x] \wedge z \in y) \\
\leftrightarrow\ & \Big\langle \text{commuting the two } \exists \Big\rangle \\
& (\exists x)(\exists y)(y = t[x] \wedge \mathscr{A}[x] \wedge z \in y) \\
\leftrightarrow\ & \Big\langle \text{one point rule (I.6.2, p. 71)} \Big\rangle \\
& (\exists x)(\mathscr{A}[x] \wedge z \in t[x])
\end{aligned}$$

Thus,[†]

$$\vdash \bigcup\{t[x] : \mathscr{A}[x]\} = \{z : (\exists x)(\mathscr{A}[x] \wedge z \in t[x])\} \tag{3}$$

□

**III.8.9 Proposition.** *The class* $\{t[x] : x \in A\}$ *($A$ a free variable) is a set, that is (using* III.8.7*),*

$$\vdash_{\mathrm{ZFC}} Coll_y((\exists x \in A)y = t[x]) \tag{4}$$

Only $x$, not $A$, is the linking variable. We could have written $\{t[x] : (x \in A)[x]\}$ to indicate this.

*Proof.* By collection,

$$\vdash_{\mathrm{ZFC}} (\exists z)(\forall x \in A)(\exists y \in z)y = t[x] \tag{5}$$

since

$$(\forall x \in A)(\exists y)y = t[x]$$

[†] Note that since we are dealing with abbreviations, this is a theorem of pure logic.

is a theorem of pure logic deduced from $t = t$ (using substitution, tautological implication, and generalization, in that order). Arguing by auxiliary constant, we add a new constant $B$ and the *assumption*

$$(\forall x)\Big(x \in A \rightarrow (\exists y)(y \in B \wedge y = t[x])\Big)$$

The one point rule and specialization yield

$$x \in A \rightarrow t[x] \in B \tag{6}$$

We can now prove that

$$\big((\exists x \in A) y = t[x]\big) \rightarrow y \in B \tag{7}$$

which will settle (4) by III.3.6.

We assume the hypothesis in (7); indeed, we go a step further: We add a new constant $C$ and the assumption

$$C \in A \wedge y = t[C]$$

Thus

$$C \in A \tag{8}$$

and

$$y = t[C] \tag{9}$$

(6) and (8) yield $t[C] \in B$. From (9), $y \in B$. □

**III.8.10 Corollary.** $\vdash_{\mathrm{ZFC}}$ $Coll_z\Big((\exists x \in A) z \in t[x]\Big)$.

*Proof.* Apply III.6.8 to $\{t[x] : x \in A\}$ (a set, by III.8.9), and use (3) above (in III.8.8). □

**III.8.11 Corollary.** $\{t[x, y] : x \in A \wedge y \in B\}$ *is a set, where A and B are free variables (and x and y are active).*

*Formally,* $\vdash_{\mathrm{ZFC}}$ $Coll_z\Big((\exists x \in A)(\exists y \in B) z = t[x, y]\Big)$.

*Proof.* We will establish

$$\vdash \{t[x, y] : x \in A \wedge y \in B\} = \bigcup \Big\{\{t[x, y] : y \in B\} : x \in A\Big\} \tag{1}$$

from which the corollary follows by two applications of III.8.9 followed by an application of union. As for (1), we transform the right hand side to the left hand side by eliminating abbreviations. The "=" instances below use III.4.1($ii$):

$$
\begin{aligned}
&\bigcup\Big\{\{t[x,y]: y \in B\}: x \in A\Big\}\\
&= \Big\langle \text{by III.8.8(3)} \Big\rangle\\
&\qquad \Big\{z : (\exists x \in A) z \in \{t[x,y] : y \in B\}\Big\}\\
&= \Big\langle \text{by III.8.7} \Big\rangle\\
&\qquad \Big\{z : (\exists x \in A)(\exists y \in B) z = t[x,y]\Big\}\\
&= \Big\langle \text{by III.8.7 again} \Big\rangle\\
&\qquad \{t[x,y] : x \in A \wedge y \in B\}
\end{aligned}
$$

□

By commutativity of ∧, (1) yields

$$\vdash \{t[x,y] : x \in A \wedge y \in B\} = \bigcup\Big\{\{t[x,y] : x \in A\} : y \in B\Big\}$$

**III.8.12 Proposition.** *In the presence of the ZFC axioms that we have introduced so far – less* collection*, except when explicitly assumed as* (1) *below – we have the following chain of implications* (*stated* conjunctively)*:* (1) → (2) → (3) → (4) → (5)*, where the statements are*

(1) *collection—version* III.8.2*,*
(2) $(\forall x)(\exists z)(\forall y)(\mathscr{P}[x,y] \to y \in z) \to (\forall A)Coll_y(\exists x \in A)\mathscr{P}[x,y]$,
(3) $(\forall x)(\exists z)(\forall y)(\mathscr{P}[x,y] \leftrightarrow y \in z) \to (\forall A)Coll_y(\exists x \in A)\mathscr{P}[x,y]$,
(4) $(\forall x)(\forall y)(\forall y')(\mathscr{P}[x,y] \wedge \mathscr{P}[x,y'] \to y = y') \to (\forall A)Coll_y(\exists x \in A)\mathscr{P}[x,y]$,
(5) $(\forall x \in A)(\exists! y)\mathscr{P}[x,y] \to (\exists z)(\forall x \in A)(\exists y \in z)\mathscr{P}[x,y]$.

*Proof.* (1) → (2): We assume (1) (collection version III.8.2). To prove (2) assume the hypothesis. Hence (specialization)

$$(\exists z)(\forall y)(\mathscr{P}[x,y] \to y \in z)$$

We add a new constant $B$ and let

$$(\forall y)(\mathscr{P}[x,y] \to y \in B) \qquad (i)$$

By III.3.6,[†]

$$Coll_y \mathscr{P}[x, y]$$

It follows that $\{y : \mathscr{P}[x, y]\}$ can be introduced formally as a set term. Hence, by III.8.10,

$$Coll_y \Big( (\exists x \in A) y \in \{y : \mathscr{P}[x, y]\} \Big)$$

In short, $Coll_y (\exists x \in A) \mathscr{P}[x, y]$; thus

$$(\forall A) Coll_y (\exists x \in A) \mathscr{P}[x, y]$$

(2) → (3): We assume (2). To prove (3), assume the hypothesis. Hence (specialization)

$$(\exists z)(\forall y)(\mathscr{P}[x, y] \leftrightarrow y \in z)$$

We add a new constant $B$ and let

$$(\forall y)(\mathscr{P}[x, y] \leftrightarrow y \in B)$$

Tautological implication followed by an invocation of ∀-monotonicity (I.4.24, p. 52) yields $(i)$ above.

(3) → (4): We assume (3). To prove (4), assume the hypothesis. Hence

$$\mathscr{P}[x, y] \wedge \mathscr{P}[x, y'] \rightarrow y = y' \tag{ii}$$

We also record the tautology

$$(\exists y) \mathscr{P}[x, y] \rightarrow (\exists y) \mathscr{P}[x, y] \tag{iii}$$

By III.2.4 (p. 122: (10), (11), (18)), $(ii)$ and $(iii)$ allow us to introduce a new function symbol, $f_{\mathscr{P}}$, into the language, and the defining axiom

$$(\exists y) \mathscr{P}[x, y] \wedge \mathscr{P}[x, f_{\mathscr{P}}[x]] \vee \neg (\exists y) \mathscr{P}[x, y] \wedge f_{\mathscr{P}}[x] = \emptyset \tag{iv}$$

into the theory. From $(iv)$ one deduces (corresponding to (19′) and (20) of III.2.4)

$$(\exists y) \mathscr{P}[x, y] \rightarrow (\mathscr{P}[x, y] \leftrightarrow y = f_{\mathscr{P}}[x]) \tag{v}$$

and

$$\neg (\exists y) \mathscr{P}[x, y] \rightarrow f_{\mathscr{P}}[x] = \emptyset \tag{vi}$$

[†] Observe how we did not need to insist that $B$ is a set. This issue was the subject of a footnote on p. 164.

We can now prove

$$(\forall x)(\exists z)(\mathscr{P}[x, y] \leftrightarrow y \in z) \tag{$vii$}$$

We have two cases:

*Case of* $(\exists y)\mathscr{P}[x, y]$. By $(v)$,

$$\mathscr{P}[x, y] \leftrightarrow y \in \{f_{\mathscr{P}}[x]\}$$

By the substitution axiom,

$$(\exists z)(\mathscr{P}[x, y] \leftrightarrow y \in z) \tag{$vii'$}$$

*Case of* $\neg(\exists y)\mathscr{P}[x, y]$. Thus, $(\forall y)\neg\mathscr{P}[x, y]$; hence $\neg\mathscr{P}[x, y]$ is derivable. By tautological implication, $\mathscr{P}[x, y] \to y \in \emptyset$.

Conversely, $y \in \emptyset \to \mathscr{P}[x, y]$ is a tautological consequence of the theorem $\neg y \in \emptyset$. Thus,

$$\mathscr{P}[x, y] \leftrightarrow y \in \emptyset$$

and we derive $(vii')$ once more, by the substitution axiom. Proof by cases now yields $(vii')$ solely on the hypothesis $(\forall x)(\forall y)(\forall y')(\mathscr{P}[x, y] \wedge \mathscr{P}[x, y'] \to y = y')$; hence we have $(vii)$ by generalization.

Having settled $(vii)$, we next obtain

$$(\forall A)Coll_y(\exists x \in A)\mathscr{P}[x, y]$$

by our hypothesis (3).

(4) → (5): We assume (4). To prove (5), assume the hypothesis, that is,

$$(\forall x \in A)(\exists! y)\mathscr{P}[x, y]$$

which entails

$$(\forall x)(x \in A \to (\exists y)\mathscr{P}[x, y]) \tag{$viii$}$$

and

$$x \in A \to \mathscr{P}[x, y] \wedge \mathscr{P}[x, y'] \to y = y' \tag{$ix$}$$

For convenience we let

$$\mathscr{Q}[x, y] \equiv x \in A \wedge \mathscr{P}[x, y] \vee x \notin A \wedge y = \emptyset$$

Work already done in III.2.4 yields, because of $(ix)$,

$$\mathscr{Q}[x, y] \wedge \mathscr{Q}[x, y'] \to y = y'$$

Thus, by hypothesis (4), we have derived

$$(\forall z)Coll_y(\exists x \in z)\mathscr{Q}[x, y]$$

Hence

$$Coll_y(\exists x \in A)\mathscr{Q}[x, y] \tag{$x$}$$

by specialization. Expanding $\mathscr{Q}$ and using the tautology

$$\Big(x \in A \wedge (x \in A \wedge \mathscr{P}[x, y] \vee x \notin A \wedge y = \emptyset)\Big) \leftrightarrow x \in A \wedge \mathscr{P}[x, y]$$

the equivalence theorem yields

$$(\exists x)\Big(x \in A \wedge (x \in A \wedge \mathscr{P}[x, y] \vee x \notin A \wedge y = \emptyset)\Big) \leftrightarrow (\exists x)(x \in A \wedge \mathscr{P}[x, y])$$

Hence, from $(x)$,

$$Coll_y(\exists x \in A)\mathscr{P}[x, y]$$

Let then (a formal definition of "$B$"[†] introduced just for notational convenience)

$$B = \{y : (\exists x)(x \in A \wedge \mathscr{P}[x, y])\} \tag{$xi$}$$

Let also $w \in A$.

By $(viii)$ we get $(\exists y)\mathscr{P}[w, y]$, which allows us to add a new constant $C$ and the assumption

$$\mathscr{P}[w, C] \tag{$xii$}$$

from which $w \in A \wedge \mathscr{P}[w, C]$ by tautological implication. Therefore

$$(\exists x)(x \in A \wedge \mathscr{P}[x, C])$$

and, by $(xi)$,

$$C \in B \tag{$xiii$}$$

Now $(xii)$ and $(xiii)$ yield $C \in B \wedge \mathscr{P}[w, C]$; thus

$$(\exists y)(y \in B \wedge \mathscr{P}[w, y])$$

The deduction theorem and hypothesis $w \in A$ yield

$$w \in A \rightarrow (\exists y \in B)\mathscr{P}[w, y]$$

[†] Of course, "$B$" is a name for a term, and what one really defines formally here is a function $f$, by $f(A, \ldots) = \{y : (\exists x)(x \in A \wedge \mathscr{P}[x, y])\}$, where "$\ldots$" are all those free variables present that we do not care to mention. In practice, "let $B$ be defined as $\ldots$" is all one really cares to say.

Hence

$$(\forall x \in A)(\exists y \in B)\mathscr{P}[x, y]$$

Thus (substitution axiom)

$$(\exists z)(\forall x \in A)(\exists y \in z)\mathscr{P}[x, y]$$

which is the conclusion part of (5). □

**III.8.13 Corollary.** *Each of the versions* (2)–(5) *of collection above is a theorem schema – hence for each specific $\mathscr{P}$ a theorem – of ZFC.* □

**III.8.14 Remark.** (I) Thus, in the sequel we may use any version of collection, as convenience dictates.

(II) Intuitively, collection versions (2)–(5) have a hypothesis that guarantees that *for each* "value" of $x$ the corresponding number of values of $y$ that satisfy $\mathscr{P}[x, y]$ is sufficiently "small" to fit into a set. In fact, in case (4) *at most* one $y$-value is possible for each $x$-value, while in case (5) *exactly one* is possible – albeit on the restriction that $x$ is varying over a set $A$. Thus, collecting *all* the values $y$, for *all* $x$ in a set $A$, yields a set under all cases (2)–(5). This set is what we call in elementary algebra or discrete mathematics courses the *image* of $A$ under the black box $\mathscr{P}[x, y]$. This black box is an agent that for each "input" value $x$ yields zero or more (but not too many) "output" values $y$.

We note that collection in its version III.8.2 does not have the "not too many" restriction on the number of outputs $y$ for each $x$, and that is why one is selective when collecting such outputs into a set. The conclusion of Axiom III.8.2,

$$(\exists z)(\forall x \in A)(\exists y \in z)\mathscr{P}[x, y]$$

allows the possibility that many outputs $y$ need *not* be included in $z$; it says only that *some* outputs are included.

(III) Collection versions (2)–(4) in III.8.12 are quite strong, even in the absence of some of the other axioms. For example, Bourbaki (1966b) adopts the axiom of pairing, but adopts collection version (2), and proves both separation and union (Exercise III.14).

Shoenfield (1967) adopts separation and proves pairing and union from collection version (3) (Exercise III.15). Finally, Levy (1979) adopts union, and proves separation and pairing from collection version (4) (Exercise III.16). □

## III.9. Axiom of Power Set

There is another operation on sets, which, intuitively, increases the size of a set "exponentially", from which fact it derives its name (see Exercise III.35 in this connection).

**III.9.1 Informal Definition (Power Class, Power Set).** For any *class* $\mathbb{A}$, $\mathbf{P}(\mathbb{A})$ stands for $\{x : \neg U(x) \wedge x \subseteq \mathbb{A}\}$. We read $\mathbf{P}(\mathbb{A})$ as *the power class of* $\mathbb{A}$.

If $A$ is a set, then $\mathbf{P}(A)$ is *also* pronounced *the power set of* $A$. □

Note that what we collect in $\mathbf{P}(\mathbb{A})$ are sets.

**III.9.2 Example (Informal).** We compute some power classes:

$$\begin{aligned}&\mathbf{P}(\emptyset) = \{\emptyset\}\\&\mathbf{P}\left(\{\emptyset\}\right) = \left\{\emptyset, \{\emptyset\}\right\}\\&\mathbf{P}\left(\{0, 1\}\right) = \left\{\emptyset, \{0\}, \{1\}, \{0, 1\}\right\}\end{aligned}$$

Also note that

(i) Since for every class $\mathbb{A}$ we have $\emptyset \subseteq \mathbb{A}$, it follows that $\emptyset \in \mathbf{P}(\mathbb{A})$.
(ii) If $a$ is a set, then $a \subseteq a$ as well; hence we have $a \in \mathbf{P}(a)$.
(iii) For a set $x$, $x \in \mathbf{P}(a)$ iff $x \subseteq a$.
(iv) Even though $U(x) \to x \subseteq a$ (is provable), still $U(x) \to x \notin \mathbf{P}(a)$ (is provable), since $x$ *must* satisfy $\neg U(x)$ for inclusion. *Power classes contain no atoms.*

**Pause.** Now $\mathbf{P}\left(\{\emptyset\}\right) \supseteq \left\{\emptyset, \{\emptyset\}\right\}$ by (i) and (ii) above. But have we not forgotten to include any other subsets of $\{\emptyset\}$? Is it really "$=$" (rather than "$\supset$") as we have claimed above? The definitive answer that one is tempted to give is "Obviously, the above is '$=$' as stated".

Well, let us prove the obvious, just to be sure:[†]

We will prove the formula $\neg U(x) \wedge x \subseteq \{\emptyset\} \to x = \emptyset \vee x = \{\emptyset\}$, that is, the tautologically equivalent

$$\neg U(x) \to x \subseteq \{\emptyset\} \to \neg x = \emptyset \to x = \{\emptyset\} \tag{1}$$

[†] My geometry teacher in high school used to say: "... [T]here are many proof methods: e.g., by contradiction, by induction, etc. Among all those proof methods the most powerful is *proof by intimidation*. It starts with the word 'obviously'. Few have the courage to challenge such a proof or to demand details ...".

Arguing by the deduction theorem, we assume the hypothesis, namely,

$$\neg U(x) \tag{2}$$

$$(\forall y)(y \in x \to y = \emptyset) \tag{3}$$

and

$$\neg x = \emptyset$$

By (2) and the above (see III.4.11)

$$(\exists y)y \in x \tag{4}$$

Let (arguing by auxiliary constant)

$$A \in x \tag{5}$$

Hypothesis (3) yields $A \in x \to A = \emptyset$. (5) now yields $A = \emptyset$; hence

$$\emptyset \in x \tag{6}$$

by the Leibniz axiom and (5). The one point rule (III.6.2, p. 149) gives

$$\vdash \emptyset \in x \leftrightarrow (\forall y)(y = \emptyset \to y \in x)$$

Thus, by (6),

$$(\forall y)(y = \emptyset \to y \in x)$$

This along with (3) yields

$$(\forall y)(y \in x \leftrightarrow y = \emptyset)$$

Thus $x = \{\emptyset\}$ (III.5.5). □

**III.9.3 Exercise.** Repeat the above argument *without* relying on the axiom of pairing. Thus, prove that

$$x \in \mathbf{P}\left(\mathbf{P}(\emptyset)\right) \leftrightarrow x = \emptyset \vee x = \mathbf{P}(\emptyset)$$

□

The following is "really true":

*If $A$ is a set, then so is* $\mathbf{P}(A)$

Indeed, let $\Sigma$ be a stage at which $A$ is formed as a set. Let $x \in \mathbf{P}(A)$, i.e., $x \subseteq A$. Every member of $x$ is available before $x$, and hence before $A$, therefore before stage $\Sigma$. Thus,

$$x \in \mathbf{P}(A) \text{ implies that } x \text{ is formed as a set at or before stage } \Sigma \tag{1}$$

Let $\Sigma'$ be a stage after $\Sigma$ (we have no problem accepting that a stage exists after a given stage). Then, by (1), $\mathbf{P}(A)$ is formed as a *set* at stage $\Sigma'$.

We could not reliably argue the above using the size limitation doctrine (Principle 3, p. 161), for it is not intuitively clear whether an "exponential growth" in set size is harmless. In fact, Principle 3 was introduced solely to justify the replacement axiom, and, in Chapter V, the axiom of infinity.

We capture the above informal argument by the following power set axiom:

**III.9.4 Axiom (Axiom of Power Set).**

$$(\exists y)(\forall x)(x \subseteq A \rightarrow x \in y) \tag{1}$$

*where $A$ is a free variable.*

Actually, the axiom as stated above is not exactly what we have established in the informal argument that preceded it. The axiom says a bit more than "the power class of a set is a set".

It is really true as stated, nevertheless. First off, the $y$ of (1) above is necessarily a set by $x \subseteq A \rightarrow x \in y$, since $(\exists x)x \subseteq A$ is provable ($A \subseteq A$ is a theorem of pure logic – see III.1.5, p. 116) and hence, so is $(\exists x)x \in y$ by $\exists$-monotonicity. Thus $\neg U(y)$ by Axiom III.1.3. We have omitted the usual qualification "$\neg U(y)$" in the statement of the axiom, since it is a conclusion that the axiom forces anyway. So the axiom says that

"There is a *set* $y$ which contains as elements all $x$ such that $x \subseteq A$, *without restricting $x$ to be a set*".

Now we see why it is really true. If $A$ is a set, then lifting the restriction from $x$ adds to $\mathbf{P}(A)$ all the urelements (see III.1.5, p. 116). Well, there *is* a set $y$ as described above, for example, $M \cup \mathbf{P}(A)$.[†]

If on the other hand $A$ is an atom, then a choice for $y$ that works is $M \cup \{\emptyset\}$.

As we have done on previous occasions, here too we prefer not to assert explicitly that the objects which our axioms claim to exist are sets (nor do we want to unnecessarily restrict our variables to be sets). We prefer to prove this

[†] We are using here the name $M$ – which was earlier introduced formally to denote the set of all atoms – to also name the set of all real atoms in the metatheory.

as a consequence of the axioms. On one hand this approach is mathematically elegant; on the other hand – more importantly – it allows us to state our axioms (e.g., power set above, as well as pairing, union, and collection) in a manner that does not betray that we allow atoms; this gives us flexibility. Thus we have chosen the statement of Axiom III.9.4 to be *morphologically* identical to the statement one would make in the absence of atoms (all variables then "vary over" sets).

**III.9.5 Proposition.**

$$\vdash_{\mathrm{ZFC}} Coll_x(\neg U(x) \wedge x \subseteq A)$$

*where A is a free variable.*

*Proof.* By (1) of III.9.4 we may assume ($B$ a new constant)

$$(\forall x)(x \subseteq A \to x \in B)$$

Hence

$$(\forall x)(\neg U(x) \wedge x \subseteq A \to x \in B) \tag{2}$$

by $\forall$-monotonicity, since

$$\models_{\mathbf{Taut}} (x \subseteq A \to x \in B) \to (\neg U(x) \wedge x \subseteq A \to x \in B)$$

We are done by III.3.6. □

We would like now to introduce the symbol "**P**" formally, in the interest of convenience, along with its informal use. As in the cases of $\cup$, $\cap$, and $\bigcup$, we will take no notational measures to distinguish between the formal and informal occurrences of the symbol; we will rely instead on the context.

**III.9.6 Definition (Formal $\mathbf{P}$).** We introduce a function symbol, $\mathbf{P}$, of arity 1, by the defining axiom

$$\mathbf{P}(A) = y \leftrightarrow (\forall x)(\neg U(x) \wedge x \subseteq A \leftrightarrow x \in y) \tag{1}$$

or, equivalently

$$(\forall x)(\neg U(x) \wedge x \subseteq A \leftrightarrow x \in \mathbf{P}(A)) \tag{2}$$

□

**III.9.7 Remark.** (I) Once again we note that it is redundant to add "$\neg U(y) \wedge$" in (1) (III.9.6) or "$\neg U(\mathbf{P}(A)) \wedge$" in (2). Indeed,

$$\vdash_{\mathrm{ZFC}} (\forall x)(\neg U(x) \wedge x \subseteq A \leftrightarrow x \in y) \leftrightarrow \neg\, U(y) \wedge \\ (\forall x)(\neg U(x) \wedge x \subseteq A \leftrightarrow x \in y)$$

To see this, note that the ← direction is a tautological implication. For the → direction we have

$$\neg U(x) \wedge x \subseteq A \leftrightarrow x \in y$$

Thus, since $\vdash_{\mathrm{ZFC}} \neg U(\emptyset) \wedge \emptyset \subseteq A$, we obtain

$$(\exists x)(\neg U(x) \wedge x \subseteq A)$$

from which $(\exists x)x \in y$ by the equivalence theorem. That is (III.1.3),

$$\neg U(y)$$

Similarly, (2) of III.9.6 proves

$$\neg U(\mathbf{P}(A)) \tag{3}$$

(II) $A$ is an arbitrary variable; thus $\mathbf{P}$ makes sense on atoms. Indeed,

$$\vdash_{\mathrm{ZFC}} U(A) \rightarrow \mathbf{P}(A) = \{\emptyset\}$$

(see Exercise III.17). □

## III.10. Pairing Functions and Products

We now turn to the *ordered pair* concept, which will lead to the formalization (within axiomatic set theory) of the intuitive concepts of *relation* and *function* in the next section. We want to invent objects "$(a, b)$" which are meaningful for all sets and atoms $a$ and $b$ and which are mindful of *order* in that

$$(a, b) = (a', b') \rightarrow a = a' \wedge b = b' \tag{1}$$

In particular, $(a, a)$ is supposed to have *two* objects in it, a *first* $a$ and a *second* $a$, so it is not to be confused with $\{a, a\} = \{a\}$.

Some naïve approaches to set theory take $(a, b)$ to be a *new kind of object* whose behaviour, i.e., (1), is "axiomatically accepted" (admittedly this is a patently odd thing to do in a *non-axiomatic* approach). To proceed formally within a framework that accepts sets and urelements as the only formal objects, we must implement our new object as a set.

There are several implementations, the simplest one (due to Kuratowski) being $\big\{\{a\},\{a,b\}\big\}$, or the related $\big\{a,\{a,b\}\big\}$.

**III.10.1 Proposition.** *If* $\big\{a,\{a,b\}\big\}=\big\{a',\{a',b'\}\big\}$*, then* $a=a'$ *and* $b=b'$*.*

*Proof.* (Presented in a “relaxed” manner, that is, in *argot*. See also III.5.9, p. 148.) By foundation, $a \neq \{a,b\}$ (otherwise $a \in a$). Thus, taking the $\subseteq$-half of the hypothesis,

$$a=a' \quad \text{and} \quad \{a,b\}=\{a',b'\} \tag{1}$$

or

$$a=\{a',b'\} \quad \text{and} \quad \{a,b\}=a' \tag{2}$$

From (2) we get $a' \in a \in a'$, contradicting foundation. Therefore, case (2) is untenable. Let us further analyze case (1), which already gives us half of what we want, namely, $a=a'$.

Thus,

$$\{a,b\}=\{a,b'\} \tag{3}$$

If $a=b$, then the $\supseteq$-part of (3) gives $b=b'$, and we are done. Otherwise, the $\subseteq$-part of (3) gives $b=b'$, and we are done again. □

The pedantic way to derive $a=a'$ goes like this: We want

$$\vdash_{\text{ZFC}} \big\{a,\{a,b\}\big\}=\big\{a',\{a',b'\}\big\} \rightarrow a=a'$$

Assume the hypothesis

$$(\forall z)(z=a \vee z=\{a,b\} \leftrightarrow z=a' \vee z=\{a',b'\})$$

Thus

$$a'=a \vee a'=\{a,b\} \leftrightarrow a'=a' \vee a'=\{a',b'\}$$

and

$$a=a \vee a=\{a,b\} \leftrightarrow a=a' \vee a=\{a',b'\}$$

Hence (by tautological implication and the axiom $x=x$)

$$a'=a \vee a'=\{a,b\} \tag{1}$$

and

$$a=a' \vee a=\{a',b'\} \tag{2}$$

which (jointly) tautologically imply

$$(a' = a \wedge a = a') \vee (a' = a \wedge a = \{a', b'\}) \\ \vee (a' = \{a, b\} \wedge a = a') \vee (a' = \{a, b\} \wedge a = \{a', b'\}) \tag{3}$$

By foundation,

$$\neg(a' = a \wedge a = \{a', b'\})$$

$$\neg(a' = \{a, b\} \wedge a = a')$$

and

$$\neg(a' = \{a, b\} \wedge a = \{a', b'\})$$

which along with (3) tautologically imply

$$a = a'$$

The rest of the above proof of III.10.1 has a straightforward formalization as a proof by cases.

**III.10.2 Definition (Pairing Function and Ordered Pair).** We introduce a new function symbol of arity 2, $J$, by

$$J(x, y) = \{x, \{x, y\}\}$$

It is customary to denote the *term* $J(x, y)$ by $(x, y)$.

We call $J(x, y)$ or $(x, y)$ *the ordered pair*. We call $J$ *the pairing function*.

"The" is dictated by our determination to have just one implementation of (ordered) pair, as that is sufficient for the theory.[†] Indeed, one seldom needs to remember how $(x, y)$ is implemented, as the property expressed in III.10.1 is all we normally need and use. □

Many of the sequel's proofs are in the "relaxed" style. We get to be formal whenever there is danger of missing fine points in this *argot*.

**III.10.3 Proposition.** *For any* $a, b, a', c'$, $(a, b) = (a', b')$ *iff* $a = a'$ *and* $b = b'$.

*Proof.* The only-if part is Proposition III.10.1. The if part follows from the Leibniz axiom. □

[†] An exception occurs in Chapter VII in our study of cardinality, where yet another pairing is considered.

Some will say that using the above definition for "pair" is overkill, since foundation was needed to establish its key property in III.10.1. By contrast, a definition of ordered pair via $\big\{\{a\}, \{a, b\}\big\}$ does not require this axiom (see Exercise III.36). This is a valid criticism for a development of set theory that is constantly preoccupied with the question of what theorem needs what axioms. In the context of our plan, it is a minor quibble, since we will seldom ask such questions, and we do have foundation anyway.

We often find it convenient to extend the notion of an ordered pair to that of an (ordered) $n$-tuple in general (for $n \geq 1$). To this end,

**III.10.4 Definition (The Ordered $n$-Tuple).** We define by induction (recursion) on $n \geq 1$ a function, $J^{(n)}$, of arity $n$:

$$J^{(1)}(x) \overset{\text{def}}{=} x \qquad \text{Basis}$$

$$J^{(n+1)}(x_1, \ldots, x_{n+1}) \overset{\text{def}}{=} J(J^{(n)}(x_1, \ldots, x_n), x_{n+1}) \qquad \text{for } n \geq 0$$

where $x, x_1, \ldots, x_{n+1}$ are variables, and $J$ is the pairing function of Definition III.10.2.

It is normal practice to denote the term $J^{(n)}(x_1, \ldots, x_n)$ – somewhat ambiguously, since the same symbol is good for any arity[†] – by the symbol

$$\langle x_1, \ldots, x_n \rangle$$

We adopt this practice henceforth and call $\langle x_1, \ldots, x_n \rangle$ an *$n$-tuple*, or *$n$-vector*, or just *vector* if $n$ is understood or unimportant. We often use the shorthand notation $\langle \vec{x}_n \rangle$ (or $\langle \vec{x} \rangle$ if $n$ is not important) for the $n$-tuple. □

**III.10.5 Remark.** (1) Some authors will not define $n$-tuples for arbitrary $n$ – once again avoiding the set $\mathbb{N}$ and inductive definitions – instead, they will "unwind" the recursion and give a definition that goes, say, up to a 5-tuple, e.g.,

$$\begin{aligned} J^{(1)}(x) &= x \\ J^{(2)}(x, y) &= J(J^{(1)}(x), y) \\ J^{(3)}(x, y, z) &= J(J^{(2)}(x, y), z) \\ &\vdots \end{aligned}$$

and leave the rest up to the imagination, invoking "...". The reader should not forget that we are using $n$ in the *metalanguage*. As far as the formal system is

[†] A "real-life" function of non-fixed arity is the *print* function of computer programming.

concerned, "$n$" of $\langle \vec{x}_n \rangle$ is *hidden in the name* – it is not a variable accessible to the formal system.

(2) Following the definition, let us compute $\langle a, b\rangle$ using the shorthand $(a, b)$ for $J(a, b)$ below:

$$\begin{aligned}\langle a, b\rangle &= (\langle a\rangle, b) \quad \text{by the induction step}\\ &= (a, b) \quad \text{by the basis step}\end{aligned}$$

Thus, from now on we denote the ordered pair by the symbol "$\langle a, b\rangle$", rather than "$(a, b)$", in the interest of notational uniformity.

(3) The ordered pair provides, intuitively, a *pairing function* – which motivates the name we gave $J$ – that, for any two objects $a$ and $b$, given in that order, "codes" them into a unique object $c$ ( $= \langle a, b\rangle$) in such a way that if, conversely, *we know* that a given $c$ is a "code", then we can *uniquely* (by III.10.3) "decode" it into $a$ and $b$. That is, if $c$ is an ordered pair, then $(\exists! x)(\exists! y)\langle x, y\rangle = c$ holds. The unique $x$ is called *the first projection* and the unique $y$ is called *the second projection* of $c$ – in symbols (we are using notation due to Moschovakis), $\pi(c)$ and $\delta(c)$ respectively.[†] More accurately, since not all sets (and no urelements) are valid "codes" (that is pairs; e.g., $\{0\}$ is not), we must let $\pi$ and $\delta$ "return" some standard "output" when the input $c$ is "bad" (not a pair).[‡] □

Let us do this formally: We record the tautology

$$(\exists x)(\exists y)\langle x, y\rangle = z \to (\exists x)(\exists y)\langle x, y\rangle = z \tag{1}$$

We next prove

$$(\exists y)\langle x, y\rangle = z \wedge (\exists y)\langle v, y\rangle = z \to x = v \tag{2}$$

Assume the hypothesis, and add the assumptions (by auxiliary constant)

$$\langle x, A\rangle = z$$

and

$$\langle v, B\rangle = z$$

Hence

$$\langle x, A\rangle = \langle v, B\rangle$$

[†] Presumably, $\pi$ for "$\pi\rho\acute{\omega}\tau\eta$" (= first) and $\delta$ for "$\delta\varepsilon\acute{\upsilon}\tau\varepsilon\rho\eta$" (= second).

[‡] Once again we will ensure that the defined function symbols, $\pi$ and $\delta$, have *total* interpretations. This determination was also at play when we defined power set and, earlier on, the formal "$\cap$", "$\cup$", and difference. We defined all these functions to act on all sets or atoms.

Therefore

$$x = v$$

by III.10.3.

**III.10.6 Definition (The First Projection $\pi$).** By the techniques found in III.2.4 (p. 122: (10), (11), (18)) we may now introduce a new function symbol $\pi$ of arity 1 by the axiom (we insert redundant brackets to avoid any misunderstanding)

$$\Big(\big((\exists x)(\exists y)\langle x,y\rangle = z\big) \wedge (\exists y)\langle \pi(z),y\rangle = z\Big) \vee \\ \Big(\big(\neg(\exists x)(\exists y)\langle x,y\rangle = z\big) \wedge \pi(z) = \emptyset\Big) \qquad \square$$

By III.2.4 (19), (20), and (19′) one directly obtains in ZFC (using III.10.6):

**III.10.7 Proposition.**

$$(\exists x)(\exists y)\langle x, y\rangle = z \to (\exists y)\langle \pi(z), y\rangle = z \qquad (\pi\text{-}19)$$

$$\neg(\exists x)(\exists y)\langle x, y\rangle = z \to \pi(z) = \emptyset \qquad (\pi\text{-}20)$$

*and*

$$(\exists x)(\exists y)\langle x, y\rangle = z \to \Big((\exists y)\langle x, y\rangle = z \leftrightarrow x = \pi(z)\Big) \qquad (\pi\text{-}19')$$

A similar analysis, which we do not repeat, yields for $\delta$:

**III.10.8 Definition (The Second Projection $\delta$).** By the techniques in III.2.4 (p. 122: (10), (11), (18)) we may now introduce a new function symbol $\delta$ of arity 1 by the axiom

$$\Big(\big((\exists x)(\exists y)\langle x, y\rangle = z\big) \wedge (\exists x)\langle x, \delta(z)\rangle = z\Big) \vee \\ \Big(\big(\neg(\exists x)(\exists y)\langle x, y\rangle = z\big) \wedge \delta(z) = \emptyset\Big) \qquad \square$$

**III.10.9 Proposition.** *The following are theorems in the presence of the defining axiom* III.10.8*:*

$$(\exists x)(\exists y)\langle x, y\rangle = z \to (\exists x)\langle x, \delta(z)\rangle = z \qquad (\delta\text{-}19)$$

$$\neg(\exists x)(\exists y)\langle x, y\rangle = z \to \delta(z) = \emptyset \qquad (\delta\text{-}20)$$

*and*

$$(\exists x)(\exists y)\langle x, y\rangle = z \rightarrow \Big((\exists x)\langle x, y\rangle = z \leftrightarrow y = \delta(z)\Big) \tag{$\delta$-19$'$}$$

It is also notationally convenient to introduce the predicate "is an ordered pair" by:

**III.10.10 Definition.** We introduce "*OP*", a predicate of arity 1, by

$$OP(z) \leftrightarrow (\exists x)(\exists y)\langle x, y\rangle = z$$

We pronounce *OP(z)* as "$z$ is an ordered pair". □

We have at once:

**III.10.11 Proposition.** *The following are* ZFC *theorems (in the presence of the appropriate defining axioms):*

$$OP(z) \rightarrow \langle \pi(z), \delta(z)\rangle = z \tag{1}$$

*and*

$$\neg OP(z) \rightarrow \pi(z) = \emptyset \wedge \delta(z) = \emptyset \tag{2}$$

*Proof.* (2) is a direct consequence of III.10.7 and III.10.9 (($\pi$-20) and ($\delta$-20)). As for (1), assume the hypothesis, *OP*($z$). By III.10.7 ($\pi$-19),

$$(\exists y)\langle \pi(z), y\rangle = z$$

while by III.10.9 ($\delta$-19),

$$(\exists x)\langle x, \delta(z)\rangle = z$$

The above two allow us to assume (where $A$ and $B$ are new constants)

$$\langle \pi(z), A\rangle = z$$

and

$$\langle B, \delta(z)\rangle = z \tag{3}$$

Hence

$$\langle \pi(z), A\rangle = \langle B, \delta(z)\rangle$$

from which $A = \delta(z)$ and $B = \pi(z)$ by III.10.3. Thus, $\langle \pi(z), \delta(z)\rangle = z$. □

It is also worth recording that

**III.10.12 Corollary.** *The following are* ZFC *theorems (in the presence of the appropriate defining axioms):*

$$\pi\big(\langle x, y\rangle\big) = x \tag{3}$$

*and*

$$\delta\big(\langle x, y\rangle\big) = y \tag{4}$$

*Proof.* We note the logical theorem $\langle x, y\rangle = \langle x, y\rangle$, from which the substitution axiom yields $(\exists u)(\exists v)\langle u, v\rangle = \langle x, y\rangle$, that is,

$$OP\big(\langle x, y\rangle\big) \tag{5}$$

For (3), III.10.7 ($\pi$-19$'$) yields (note dummy renaming)

$$OP\big(\langle x, y\rangle\big) \rightarrow \Big((\exists u)\langle x, u\rangle = \langle x, y\rangle \leftrightarrow x = \pi\big(\langle x, y\rangle\big)\Big) \tag{6}$$

By (5) and the logical theorem $(\exists u)\langle x, u\rangle = \langle x, y\rangle$, (6) yields

$$x = \pi\big(\langle x, y\rangle\big)$$

The case for $\delta$ is similar. □

In recursion theory (or *computability*, studied in volume 1), pairing functions on the natural numbers play an important role. There are several so-called *primitive recursive* pairing functions, e.g., $2^x 3^y$, $2^x(2y + 1)$, $2^{x+y+2} + 2^{y+1}$, $(x + y)^2 + x$, $(x + y)(x + y + 1)/2 + x$. Of these, only the last one ensures that every $n \in \mathbb{N}$ is a “pair”, while the second one misses only the number 0.

**III.10.13 Proposition.** *For $n \geq 2$ and any objects $a_1, \ldots, a_n$, $\langle \vec{a}_n\rangle$ is a set.*

*Proof.* Exercise III.38. □

**III.10.14 Proposition.** *For $n \geq 1$ and any objects $a_1, \ldots, a_n, b_1, \ldots, b_n$,*

$$\langle \vec{a}_n\rangle = \langle \vec{b}_n\rangle \quad \textit{iff} \quad a_i = b_i \textit{ for } i = 1, \ldots, n$$

*Proof.* Exercise III.39. □

**III.10.15 Informal Definition (The Cartesian Product of Two Classes).** For any classes $\mathbb{A}$ and $\mathbb{B}$, the symbol $\mathbb{A} \times \mathbb{B}$, read the *Cartesian product of* $\mathbb{A}$ *and* $\mathbb{B}$ (in that order), is an abbreviation for the class term $\{\langle a, b\rangle : a \in \mathbb{A} \wedge b \in \mathbb{B}\}$ (see also III.8.7). □

**III.10.16 Lemma.** $\{\langle x, y\rangle : \mathscr{T}[x, y]\} = \{z : OP(z) \wedge \mathscr{T}[\pi(z), \delta(z)]\}$ *is a theorem schema.*

*Proof.* By III.8.7 the left hand side abbreviates the class term

$$\{z : (\exists x)(\exists y)(\langle x, y\rangle = z \wedge \mathscr{T}[x, y])\}$$

Thus we need to prove

$$(\exists x)(\exists y)(\langle x, y\rangle = z \wedge \mathscr{T}[x, y]) \leftrightarrow OP(z) \wedge \mathscr{T}[\pi(z), \delta(z)] \tag{1}$$

We note the theorem

$$\langle x, y\rangle = z \leftrightarrow OP(z) \wedge \pi(z) = x \wedge \delta(z) = y \tag{2}$$

Indeed, the → direction is by the Leibniz axiom and

$$OP(\langle x, y\rangle) \wedge \pi(\langle x, y\rangle) = x \wedge \delta(\langle x, y\rangle) = y$$

from the definition of $OP$ and III.10.12. The ← direction is by III.10.11.

Now (2) yields, via the equivalence theorem, the first equivalence of the following "calculation":

$$\begin{aligned}
&(\exists x)(\exists y)(\langle x, y\rangle = z \wedge \mathscr{T}[x, y])\\
\leftrightarrow\ &\Big\langle \text{see above} \Big\rangle\\
&(\exists x)(\exists y)(OP(z) \wedge \pi(z) = x \wedge \delta(z) = y \wedge \mathscr{T}[x, y])\\
\leftrightarrow\ &\Big\langle \text{no free } x, y \text{ in } OP(z) \Big\rangle\\
&OP(z) \wedge (\exists x)(\exists y)(\pi(z) = x \wedge \delta(z) = y \wedge \mathscr{T}[x, y])\\
\leftrightarrow\ &\Big\langle \text{one point rule} \Big\rangle\\
&OP(z) \wedge (\exists x)(\pi(z) = x \wedge \mathscr{T}[x, \delta(z)])\\
\leftrightarrow\ &\Big\langle \text{one point rule} \Big\rangle\\
&OP(z) \wedge \mathscr{T}[\pi(z), \delta(z)])
\end{aligned}$$

We have proved (1). □

**III.10.17 Theorem.** *For any variables $A$ and $B$, $A \times B$ is a set.*

*Proof.* By III.8.11 (p. 172), $\vdash_{\mathrm{ZFC}} Coll_z\big((\exists x)(\exists y)(z = \langle x, y\rangle \wedge x \in A \wedge y \in B)\big)$ for any free variables $A$ and $B$. □

Using the recently introduced symbols and III.10.16,

$$\vdash_{\text{ZFC}} Coll_z\big(OP(z) \wedge \pi(z) \in A \wedge \delta(z) \in B\big)$$

Thus, we might as well introduce the formal "×":

**III.10.18 Definition (Formal $\times$).** In view of the above observation, we introduce a new function symbol, $\times$, of arity 2 by the defining axiom

$$A \times B = y \leftrightarrow \neg U(y) \wedge (\forall z)(z \in y \leftrightarrow OP(z) \wedge \pi(z) \in A \wedge \delta(z) \in B)$$

or

$$A \times B = \{z : OP(z) \wedge \pi(z) \in A \wedge \delta(z) \in B) \qquad \square$$

This $A \times B$ makes sense for all variables $A$ and $B$. In particular, one can prove

$$U(A) \rightarrow A \times B = \emptyset$$

as well as

$$\emptyset \times B = \emptyset$$

**III.10.19 Remark.** The following proof of III.10.17 for any *sets* $A$ and $B$ is often criticized as overkill (e.g., Barwise (1975)), while Bourbaki (1966b), Levy (1979), and Shoenfield (1967) – who use the collection-based proof above – but not Jech (1978b), just stay away from it without comment:

Let $\langle a, b\rangle \in A \times B$, i.e., $a \in A$ and $b \in B$. Thus, $\{a, b\} \subseteq A \cup B$, and therefore $\{a, b\} \in \mathbf{P}(A \cup B)$. It follows that $\big\{a, \{a, b\}\big\} \subseteq A \cup \mathbf{P}(A \cup B)$ and hence

$$\big\{a, \{a, b\}\big\} \in \mathbf{P}\left(A \cup \mathbf{P}(A \cup B)\right)$$

Thus $\langle a, b\rangle \in \mathbf{P}\left(A \cup \mathbf{P}(A \cup B)\right)$, establishing $A \times B \subseteq \mathbf{P}\left(A \cup \mathbf{P}(A \cup B)\right)$. By separation, $A \times B$ is a set.

An additional criticism here may be that this proof needed to know the implementation of "$\langle a, b\rangle$", while the one, based on collection, does not need this information.

The objection that the proof is overkill, on the other hand, is context-dependent. If the foundation of set theory is going to exclude the power set axiom (one important set theory so restricted is that of Kripke and Platek with or without urelements – "KP" or "KPU"; e.g., Barwise (1975)), then the objection is justified. If on the other hand we do have the power set axiom, then we certainly are going to take advantage of it, and we reserve the right to use any axiom we please in our proofs. □

**III.10.20 Example (Informal).** $\{0\} \times \{1\} = \{\langle 0, 1\rangle\}$ and $\{1\} \times \{0\} = \{\langle 1, 0\rangle\}$. Since $\langle 0, 1\rangle \neq \langle 1, 0\rangle$, these two products are different; hence $\mathbb{A} \times \mathbb{B} \neq \mathbb{B} \times \mathbb{A}$ in general. □

We conclude this section by extending (more *argot*) $\times$ to any finite number of class "operands", just as we did for $\cup$ and $\cap$ in III.4.15 (p. 142).

**III.10.21 Informal Definition.** Given classes $\mathbb{A}_i$ for $i = 1, \ldots, n$,

$$\bigtimes_{i=1}^{n} \mathbb{A}_i \quad \text{and} \quad \bigtimes\nolimits_{i=1}^{n} \mathbb{A}_i \quad \text{and} \quad \bigtimes_{1 \le i \le n} \mathbb{A}_i$$

are alternative abbreviations for

$$\{\langle \vec{x}_n \rangle : x_1 \in \mathbb{A}_1 \wedge \cdots \wedge x_n \in \mathbb{A}_n\} \tag{$*$}$$

We avoid "$\cdots$" by the inductive definition

$$\bigtimes_{i=1}^{1} \mathbb{A}_i \text{ stands for } \mathbb{A}_1$$

$$\bigtimes_{i=1}^{n+1} \mathbb{A}_i \text{ stands for } \Big(\bigtimes_{i=1}^{n} \mathbb{A}_i\Big) \times \mathbb{A}_{n+1}$$

One often writes $\mathbb{A}_1 \times \cdots \times \mathbb{A}_n$ rather than $\bigtimes\nolimits_{i=1}^{n} \mathbb{A}_i$.

If all the $\mathbb{A}_i$ are equal, say to $\mathbb{A}$, then we will usually write $\mathbb{A}^n$. We let $\mathbb{A}^1$ mean $\mathbb{A}$. □

That the "$\ldots$" notation, in $(*)$ of III.10.21 above, and the inductive definition coincide can be verified using III.10.4.

We can, of course, use the metalogical "=" in lieu of "stands for". For example, the logical theorem $\mathbb{A}_1 = \mathbb{A}_1$ leads to the logical theorem $\bigtimes\nolimits_{i=1}^{1} \mathbb{A}_i = \mathbb{A}_1$ on replacing the left $\mathbb{A}_1$ by the "abbreviation" $\bigtimes\nolimits_{i=1}^{1} \mathbb{A}_i$.

**III.10.22 Informal Definition.** We often have a "rule" which for each $a \in \mathbb{I}$ "gives" us a class $\mathbb{A}_a$. This simply means that for some formula $\mathscr{A}(x, y)$ (the "rule") we *consider*[†] the classes $\{x : \mathscr{A}(a, x)\}$ for each $a \in \mathbb{I}$. $\mathbb{I}$ is the *index class*.

We cannot in general collect all the $\mathbb{A}_a$ into a class, yet we can (informally) "define" their union and intersection:

$$\bigcup_{a\in\mathbb{I}} \mathbb{A}_a \text{ stands for } \{x : (\exists a \in \mathbb{I})x \in \mathbb{A}_a\} \text{ that is,} \{x : (\exists a \in \mathbb{I})\mathscr{A}(a, x)\}$$

and

$$\bigcap_{a\in\mathbb{I}} \mathbb{A}_a \text{ stands for } \{x : (\forall a \in \mathbb{I})x \in \mathbb{A}_a\} \text{ that is,} \{x : (\forall a \in \mathbb{I})\mathscr{A}(a, x)\}$$

The case $\mathbb{I} = \mathbb{N}$ occurs frequently in informal discussions. □

**III.10.23 Proposition.** *If for $n \geq 2$ all of $A_1, \ldots, A_n$ are sets, then so is $A_1 \times \cdots \times A_n$.*

*Proof.* By III.10.21 and induction on $n$.[‡] □

**III.10.24 Corollary.** *For any set $A$, $A^n$ is a set for $n \geq 1$.*

## III.11. Relations and Functions

We intuitively picture a *binary relation* as a table of rows,[§] each row containing two objects, a first object (occupying the first column) and a second object (occupying the second column) – see also Section I.2, p. 20.

A table naturally leads to a (usually) *one-to-many* "rule" that to each object from some class *associates* one or more[¶] elements from another (possibly the same) class: Simply associate to the the first object on each row (the *input object*) the second object of the row (the *output object*).

Conversely any *one-to-many* "rule", regardless of how it is expressed (regardless of *intention*) can be represented as a table by forming a class of rows where the second object in each row is associated to the first, according to the given rule.

[†] "Consider", not "collect", since some $\mathbb{A}_a$ may be proper classes and we are unwilling to collect other than sets or atoms into a class.

[‡] This is a "theorem schema". For each value of the informal object $n$ we have a (different) theorem: "$A \times B$ is a set"; "$A \times B \times C$ is a set"; etc. We have suggested above a (meta)proof of all these theorems at once by induction in the metatheory.

[§] Such a table may have, intuitively, infinite length.

[¶] Hence the term "one-to-many".

Our rigorous counterpart of a rule or table is then a class of ordered pairs.[†] Such a class is what we call a *binary relation*, or just *relation*.

**III.11.1 Informal Definition (Binary Relations).** A *binary relation*, or just *relation*, is a class $\mathbb{T}$ whose members are (exclusively) ordered pairs.

*Within* ZFC, that "$\mathbb{T}$ is a relation" is *argot* for "$z \in \mathbb{T} \to OP(z)$ is a theorem". Similarly, "let $\mathbb{T}$ be a relation" means "add the assumption $z \in \mathbb{T} \to OP(z)$".

If $\mathbb{T}$ is a relation, then the notations $\langle a, b\rangle \in \mathbb{T}$ and $b\,\mathbb{T}\,a$ (*note the order reversal in the notation*) mean exactly the same thing.

A relation $\mathbb{T}$ often is introduced as a class term $\{\langle x, y\rangle : \mathscr{T}[x, y]\}$ or, equivalently (III.10.16), $\{z : OP(z) \wedge \mathscr{T}[\pi(z), \delta(z)]\}$.

We call $\mathscr{T}$ the *defining formula* of the relation $\mathbb{T}$. In most practical cases $\mathscr{T}$ has no *parameters*, that is, $x$ and $y$ are its only free variables. In such cases we say that $\mathbb{T}$ is the *relational implementation* of $\mathscr{T}(x, y)$ or that it is *the relational extension of* $\mathscr{T}(x, y)$. □

**III.11.2 Remark.** (1) The term "binary", *understood if omitted*, refers to the fact that we have a class of (ordered) *pairs* in mind.

Some mathematicians – especially in the context of a discrete mathematics course – want to have *n-ary* relations, for any $n \geq 1$, that is, classes whose members are $n$-tuples (III.10.4, p. 185). We will not spend any nontrivial amount of time on those, since for any $n \geq 2$, $\langle \vec{x}_n\rangle = \langle\langle \vec{x}_{n-1}\rangle, x_n\rangle$ (by III.10.4), and therefore any $n$-ary relation, for $n \geq 2$, is a *binary* relation. For $n = 1$ we have the *unary* relations, that is, classes of elements that are 1-tuples, $\langle x\rangle$. Since $\langle x\rangle = x$ (cf. III.10.4), unary relations are just classes with no additional requirements imposed on their elements. We will not use the terminology "unary relations"; rather we will just call them classes (or sets, as the case may be). For the record, when one uses $n$-ary relations, one usually abbreviates "$\langle \vec{x}_n\rangle \in \mathbb{T}$" by "$\mathbb{T}(\vec{x}_n)$". In particular, when $n = 2$, the texts "$\langle x, y\rangle \in \mathbb{T}$", "$\mathbb{T}(x, y)$" and "$y\,\mathbb{T}\,x$" state the same thing.

An $n$-ary relation $\mathbb{T}$ may naturally arise as the *extension* or *implementation* of a formula of $n$ free variables, that is, as $\mathbb{T} = \{\langle \vec{x}_n\rangle : \mathscr{T}(\vec{x}_n)\}$ (see III.8.7). In this case, and in view of the above comment, the texts "$\mathbb{T}(\vec{x}_n)$" and "$\mathscr{T}(\vec{x}_n)$" are interchangeable in the *argot* of $n$-ary relations.

(2) The empty set is obviously a relation.

(3) Note the reversal of order in "$\langle a, b\rangle \in \mathbb{T}$ iff $b\,\mathbb{T}\,a$" in III.11.1. This is one of a variety of tricks employed in the literature in order to make notation

[†] Much is to be gained in notational convenience if we do not restrict relations to be sets.

regarding *composition* consistent between relations and functions (we will return to clarify this point when composition is introduced). The trick employed here is as in Shoenfield (1978); for a different one see Levy (1979).

(4) In the same spirit, whenever the defining formula $\mathscr{F}$ of a relation $\mathbb{F}$ is by convention written in so-called *infix* notation (i.e., $x \mathscr{F} y$) rather than *prefix* (i.e., $\mathscr{F}(x, y)$) – e.g., one writes $x < y$ rather than $<(x, y)$ – then we observe this reversal by writing $\mathbb{F} = \{\langle y, x\rangle : x \mathscr{F} y\}$ or $\mathbb{F} = \{z : OP(z) \wedge \delta(z) \mathscr{F} \pi(z)\}$. This notation has the nice side effect that $a \,\mathbb{F}\, b \leftrightarrow a \mathscr{F} b$ is provable. For example, $\{\langle y, x\rangle : x < y)\}$ is the relational implementation of the formula $x < y$.

**Note.** We will continue writing $\mathbb{F} = \{\langle x, y\rangle : \mathscr{F}(x, y)\}$, that is, there is *no reversal* of variables if the defining formula $\mathscr{F}$ is written in the usual prefix notation.

Whenever $b \,\mathbb{T}\, a$ holds, we say that $\mathbb{T}$, when presented with *input* $a$, "responds" with $b$ among its (possibly many different) *outputs*.

(5) A relation often inherits the *name* of the defining formula. Thus the relation $\{\langle y, x\rangle : x \in y\}$ is also denoted by "$\in$", and $\langle y, x\rangle \in \, \in$ means $x \in y$. The left "$\in$" in "$\langle y, x\rangle \in \, \in$" is the nonlogical symbol, while the right "$\in$" is the informal name of the relation that *extends* the formula $x \in y$. Similarly, $<$ is used as both the name of $\{\langle y, x\rangle : x < y\}$ and that of the defining formula; thus $\langle y, x\rangle \in \, <$ means $x < y$.

With some practice, all this will be less confusing than at first sight. □

**III.11.3 Example (Informal).** Here are some relations: $\emptyset$, $\{\langle 0, 1\rangle\}$, $\mathbb{R}^2$ (where $\mathbb{R}$ is the set of all reals), $\{\langle 0, 1, 2\rangle\}$. According to the above remark, the last example is both 3-ary (ternary) and binary, since $\langle 0, 1, 2\rangle = \langle\langle 0, 1\rangle, 2\rangle$. □

**III.11.4 Informal Definition.** Let $\mathbb{S}$ be any class (binary relation or not).

dom($\mathbb{S}$), its *domain*, is an *abbreviation* for the class $\{x : (\exists y)\langle x, y\rangle \in \mathbb{S}\}$ or $\{\pi(z) : OP(z) \wedge z \in \mathbb{S}\}$, i.e., the class of *all* "useful" inputs – those which do "cause" some output *in* $\mathbb{S}$. The *range* of $\mathbb{S}$, ran($\mathbb{S}$), on the other hand stands for the class of *all* the outputs "caused" by all inputs *in* $\mathbb{S}$. In symbols, $\{y : (\exists x)\langle x, y\rangle \in \mathbb{S}\}$ or, equivalently, $\{\delta(z) : OP(z) \wedge z \in \mathbb{S}\}$.

*The* argot *concepts "*dom*" and "*ran*" apply, in particular, to relations* $\mathbb{S}$.

The class that contains all the useful inputs *and* all the outputs is the *field* of the class $\mathbb{S}$, that is, dom($\mathbb{S}$) $\cup$ ran($\mathbb{S}$).

If $\mathbb{S} \subseteq \mathbb{A} \times \mathbb{B}$ for some $\mathbb{A}$ and $\mathbb{B}$, then we say that "$\mathbb{S}$ *is a relation on* $\mathbb{A} \times \mathbb{B}$" or that "$\mathbb{S}$ *is a relation from* $\mathbb{A}$ *to* $\mathbb{B}$" or that "$\mathbb{S}$ *is a relation that maps* $\mathbb{A}$ *into*

$\mathbb{B}$”. The symbol[†] $\mathbb{S} : \mathbb{A} \to \mathbb{B}$ is read exactly like any one of the three previous italicized sentences in quotes.

$\mathbb{A}$ is called the *left field* and $\mathbb{B}$ is called the *right field* of $\mathbb{S}$.

If $\mathbb{S} \subseteq \mathbb{A} \times \mathbb{A}$, then we say that $\mathbb{S}$ *is a relation on* $\mathbb{A}$ rather than on $\mathbb{A} \times \mathbb{A}$.

Given $\mathbb{S} : \mathbb{A} \to \mathbb{B}$ and *in the context of these fields*, $\mathbb{S}$ is *total* iff $\mathrm{dom}(\mathbb{S}) = \mathbb{A}$; otherwise it is *nontotal*.

It is *onto* iff $\mathrm{ran}(\mathbb{S}) = \mathbb{B}$. In this case we often say that $\mathbb{S}$ *maps* $\mathbb{A}$ *onto* $\mathbb{B}$, or just *that* $\mathbb{S}$ *is onto* $\mathbb{B}$.

The *converse* or *inverse* of any class $\mathbb{S}$, in symbols $\mathbb{S}^{-1}$, is the class $\{\langle x, y\rangle : \langle y, x\rangle \in \mathbb{S}\}$.

The concept of inverse (converse) applies, in particular, to relations $\mathbb{S}$.

Let $\mathbb{S} : \mathbb{A} \to \mathbb{B}$, $\mathbb{X} \subseteq \mathbb{A}$, and $\mathbb{Y} \subseteq \mathbb{B}$. The *image* of $\mathbb{X}$ under $\mathbb{S}$, in symbols $\mathbb{S}[\mathbb{X}]$, is the class of all the outputs that are caused by inputs in $\mathbb{X}$, i.e., $\{y : (\exists x \in \mathbb{X})y\,\mathbb{S}\,x\}$.

We have the *non*-standard[‡] shorthand $\mathbb{S}\langle c\rangle$ for $\mathbb{S}[\{c\}]$.

The *inverse image* of $\mathbb{Y}$ under $\mathbb{S}$ is just $\mathbb{S}^{-1}[\mathbb{Y}]$.

We have the *non*-standard shorthand $\mathbb{S}^{-1}\langle c\rangle$ for $\mathbb{S}^{-1}[\{c\}]$. □

**III.11.5 Remark.** (1) The notions of left field and right field are not absolute; they depend on the context. It is clear that once left and right fields are chosen, then any super-class of the left (respectively, the right) field is also a left (respectively, right) field. Conversely, one can always narrow the left field until it equals $\mathrm{dom}(\mathbb{S})$, thus rendering $\mathbb{S}$ total. A similar comment holds for the concept of *onto*. That may create the impression that the notions “total”, “nontotal”, and “onto” are really useless.

This is not so, for in many branches of mathematics the studied relations and functions have “natural” associated classes (usually sets) from which inputs are taken and into which outputs are placed. For example, in (ordinary) recursion theory functions take inputs from $\mathbb{N}$ and produce outputs in $\mathbb{N}$. It is a (provably) unsolvable problem of that theory to determine for any given such function, *in general*, whether it is total or onto.[§] Therefore it is out of the question to make[¶] left and right fields “small enough” to render the arbitrary such function total and onto.

[†] The context will not allow confusion between the logical → and the one employed, as is the case here, to mean “to”.

[‡] A reason for its being non-standard becomes obvious as soon as we consider III.11.14.

[§] By Rice’s theorem, proved in volume 1.

[¶] “Make” with the tools of recursion theory, that is. Such tools are formalized algorithms.

(2) Note that for any $a$ and $b$, $b \in \mathbb{S}\langle a\rangle$ iff $b \in \mathbb{S}[\{a\}]$ iff $(\exists x \in \{a\}) b\,\mathbb{S}\,x$ iff $(\exists x)(x = a \wedge b\,\mathbb{S}\,x)$ iff $b\,\mathbb{S}\,a$. This pedantic (conjunctional) iff chain proves (within pure logic, where we wrote the *argot* "iff" for "$\leftrightarrow$") the obvious

$$b \in \mathbb{S}\langle a\rangle \leftrightarrow b\,\mathbb{S}\,a \tag{$i$}$$

Similarly,

$$b \in \mathbb{S}^{-1}\langle a\rangle \leftrightarrow b\,\mathbb{S}^{-1}\,a \tag{$ii$}$$

since $\mathbb{S}^{-1}$ is a relation.

(3) The definition (III.11.4) of inverse relation is equivalent to

$$b\,\mathbb{S}\,a \quad \text{iff} \quad a\,\mathbb{S}^{-1}\,b$$

Using $(i)$ and $(ii)$, we obtain at once

$$\vdash b \in \mathbb{S}\langle a\rangle \leftrightarrow a \in \mathbb{S}^{-1}\langle b\rangle$$

(4)

$$\vdash \mathbb{S}[\mathbb{X}] = \bigcup\{\mathbb{S}\langle x\rangle : x \in \mathbb{X}\}$$

as the following calculation shows.

$$\begin{aligned}
\bigcup\{\mathbb{S}\langle x\rangle : x \in \mathbb{X}\} &= \Big\{z : (\exists x)(x \in \mathbb{X} \wedge z \in \mathbb{S}\langle x\rangle)\Big\} && \text{(by III.8.8)}\\
&= \Big\{z : (\exists x)(x \in \mathbb{X} \wedge z\,\mathbb{S}\,x)\Big\} && \text{(by $(i)$ above)}\\
&= \mathbb{S}[\mathbb{X}] && \text{(Definition III.11.4)}
\end{aligned}$$

(5)

$$\vdash \mathbb{S}^{-1}[\mathbb{Y}] = \{x : \mathbb{Y} \cap \mathbb{S}\langle x\rangle \neq \emptyset\}$$

as the following calculation shows:

$$\begin{aligned}
\mathbb{S}^{-1}[\mathbb{Y}] &= \{x : (\exists y \in \mathbb{Y}) x\,\mathbb{S}^{-1} y\}\\
&= \{x : (\exists y)(y \in \mathbb{Y} \wedge y\,\mathbb{S}\,x)\}\\
&= \{x : (\exists y)(y \in \mathbb{Y} \wedge y \in \mathbb{S}\langle x\rangle)\}\\
&= \{x : (\exists y)(y \in \mathbb{Y} \cap \mathbb{S}\langle x\rangle)\}\\
&= \{x : \mathbb{Y} \cap \mathbb{S}\langle x\rangle \neq \emptyset\}
\end{aligned}$$

□

**III.11.6 Example (Informal).** Let $S = \{\langle 0, a\rangle, \langle 0, b\rangle, \langle 1, c\rangle, \langle\{0, 1\}, a\rangle\}$. Then $S\langle 0\rangle = S[\{0\}] = \{a, b\}$, $S[\{0, 1\}] = \{a, b, c\}$. On the other hand, $S\langle\{0, 1\}\rangle = S[\{\{0, 1\}\}] = \{a\}$. Thus, $S[\{0, 1\}] \neq S\langle\{0, 1\}\rangle$.

This phenomenon occurs because $\mathrm{dom}(S)$ has a member, namely $\{0, 1\}$, which is also a subset of $\mathrm{dom}(S)$. One encounters a lot of sets like this in set theory, so the *common* notation "$\mathbb{S}(\mathbb{X})$", which is used in naïve approaches both for the *image* (when $\mathbb{X}$ is viewed as a collection of points) and for the output(s) when $\mathbb{X}$ is a single input ($\mathbb{X}$ now being viewed as a point), would have been ambiguous in our setting.

What does $\mathbb{S}\langle a\rangle = \emptyset$ mean? By III.4.11 it translates into $\neg(\exists x)x \in \mathbb{S}\langle a\rangle$. This is (logically) equivalent to $a \notin \{z : (\exists x)x \, \mathbb{S} \, z\}$, that is, $a \notin \mathrm{dom}(\mathbb{S})$, or $\mathbb{S}\langle a\rangle$ is *undefined*. □

**III.11.7 Example (Informal).** (1) Let $<$ and $>$ be the usual predicates on $\mathbb{N}$, and let us use the same symbols for the relational extensions of the atomic formulas $x < y$ and $x > y$. Then, $<\langle 3\rangle = \{x : x < 3\} = \{0, 1, 2\}$. Similarly, $>\langle 3\rangle = \{4, 5, 6, \ldots\}$.

(2) Let $\mathbb{M} = \{\langle 0, x\rangle : x = x\}$. Then $\mathrm{dom}(\mathbb{M}) = \{0\}$ and $\mathrm{ran}(\mathbb{M}) = \mathbb{U}_M$. Thus a relation that is a proper class *can* have a domain which is a set. Similar comment for the range (think of $\mathbb{M}^{-1}$). □

**III.11.8 Proposition.** *If the relation $S$ is a set, then so are* $\mathrm{dom}(S)$ *and* $\mathrm{ran}(S)$.

*Proof.* Assume the hypothesis. By

$$z \in S \to OP(z) \models_{\mathbf{Taut}} z \in S \leftrightarrow z \in S \wedge OP(z)$$

and III.11.4 we get $\vdash \mathrm{dom}(S) = \{\pi(z) : z \in S\}$. The claim follows now from III.8.9.

The argument for $\mathrm{ran}(S)$ just uses $\delta(z)$ instead. □

**III.11.9 Informal Definition.** For any relation $\mathbb{S}$, "$a \in \mathrm{dom}(\mathbb{S})$" is pronounced "$\mathbb{S}\langle a\rangle$ is defined". We use the symbol "$\mathbb{S}\langle a\rangle \downarrow$" to indicate this. Correspondingly, "$a \notin \mathrm{dom}(\mathbb{S})$" is pronounced "$\mathbb{S}\langle a\rangle$ is undefined". We use the symbol "$\mathbb{S}\langle a\rangle \uparrow$" to indicate this.

If $\mathbb{T}$ is a relation and $\mathbb{S} \subseteq \mathbb{T}$, then $\mathbb{T}$ is an *extension* of $\mathbb{S}$, and $\mathbb{S}$ is a *restriction* of $\mathbb{T}$.

If $\mathbb{T}$ is a relation and $\mathbb{A}$ is some class, then a *restriction of* $\mathbb{T}$ *on* $\mathbb{A}$ is usually obtained in one of two ways:

(1) Restrict *both* inputs and outputs to be in $\mathbb{A}$, to obtain $\mathbb{T} \cap \mathbb{A}^2$. The symbol $\mathbb{T} \mid \mathbb{A}$ is used as a shorthand for this restriction.
(2) Restrict *only* the inputs to be in $\mathbb{A}$, to obtain $\{x \in \mathbb{T} : \pi(x) \in \mathbb{A}\}$. This restriction is denoted by $\mathbb{T} \restriction \mathbb{A}$. □

**III.11.10 Example (Informal).** Suppose that we are working in $\mathbb{N}$. Thus $\{\langle 2,1\rangle, \langle 2,0\rangle, \langle 1,0\rangle\} = {<} \cap \{0,1,2\}^2$. It is also the case that $\{\langle 2,1\rangle, \langle 2,0\rangle, \langle 1,0\rangle\} = {<} \restriction \{0,1,2\}$, so that both versions of restricting the relation $<$ on the set $\{0,1,2\}$ give the same result.

Now, $\{\langle 1,2\rangle, \langle 0,2\rangle, \langle 0,1\rangle\} = {>} \cap \{0,1,2\}^2$. However,

$$>\restriction \{0,1,2\} = \{\langle 0,1\rangle, \langle 0,2\rangle, \ldots, \langle 1,2\rangle, \langle 1,3\rangle \ldots, \langle 2,3\rangle, \langle 2,4\rangle \ldots\}.$$

Here the two versions of restriction are not the same. □

**III.11.11 Remark.** (1) By the concluding remarks in III.11.6, $\mathbb{S}\langle a\rangle \downarrow$ iff $\mathbb{S}\langle a\rangle \neq \emptyset$, while $\mathbb{S}\langle a\rangle \uparrow$ iff $\mathbb{S}\langle a\rangle = \emptyset$.

(2) For relations $\mathbb{T}$ the most commonly used version of restriction is $\mathbb{T} \mid \mathbb{A}$. Occasionally one sees $\mathbb{T} \upharpoonleft \mathbb{A}$ for $\mathbb{T} \restriction \mathbb{A}$ (Levy (1979)).

(3) A relation $\mathbb{S} : \mathbb{A} \to \mathbb{B}$ is sometimes called a *partial multiple-valued function* from $\mathbb{A}$ to $\mathbb{B}$. "Partial" refers to the *possibility* of being nontotal, while "multiple-valued" refers to the fact that, in general, $\mathbb{S}$ can give several outputs for a given input.

Remove this possibility, and you get a (partial) *function*. □

**III.11.12 Informal Definition ((Informal) Functions).** A *function* $\mathbb{F}$ is a single-valued relation, more precisely, single-valued *in the second projection*.

If we are working in ZFC, then "$\mathbb{F}$ is single-valued in the second projection" is *argot* for

$$\text{“}x \in \mathbb{F} \wedge y \in \mathbb{F} \wedge \pi(x) = \pi(y) \to \delta(x) = \delta(y)\text{”} \tag{1}$$

Thus, "if $\mathbb{F}$ is a function, ..." adds (1) to the axioms (of ZFC), while "... $\mathbb{F}$ is a function ..." claims that (1) is a theorem.

If $\mathbb{F} : \mathbb{A} \to \mathbb{B}$, then $\mathbb{F}$ is a *partial function* from $\mathbb{A}$ to $\mathbb{B}$. The qualification "partial" will always be understood (see above remark), and therefore will not be mentioned again. □

**III.11.13 Remark.** (1) The definition of single-valuedness can also be stated as $b\,\mathbb{F}\,a \wedge c\,\mathbb{F}\,a \to b = c$ (where $a, b, c$ are free), or even $\langle a, b\rangle \in \mathbb{F} \wedge \langle a, c\rangle \in \mathbb{F} \to b = c$.

(2) Clearly, if $\mathbb{F}$ is a function,[†] then we can prove $z \in \mathbb{F} \to \mathbb{F}\langle \pi(z)\rangle = \{\delta(z)\}$ (we have $\supseteq$ by definition of $\mathbb{F}\langle x\rangle$ and $\subseteq$ by single-valuedness).

(3) $\emptyset$ is a function.

[†] We are not going to continue reminding the reader that this is *argot*. See III.11.12.

(4) Since a relation is the "implementation" of a formula as a class, so is a function. But if the relation $\mathbb{F}$, defined from the formula $\mathscr{F}(x, y)$, is a function – that is, we have the abbreviation

$$\mathbb{F} = \{\langle x, y\rangle : \mathscr{F}(x, y)\} \tag{$i$}$$

and also a proof of

$$\langle x, y\rangle \in \mathbb{F} \wedge \langle x, z\rangle \in \mathbb{F} \rightarrow y = z \tag{$ii$}$$

– then we must also be able to prove

$$\mathscr{F}(x, y) \wedge \mathscr{F}(x, z) \rightarrow y = z \tag{$iii$}$$

Indeed, we are (and a bit more).

First off, we see at once – by (slightly ab)using III.4.1($iii$)[†] (p. 134) – that "$\langle x, y\rangle \in \mathbb{F}$" abbreviates $\mathscr{F}(x, y)$.

A more serious (i.e., complete) reason is this: "$\langle x, y\rangle \in \mathbb{F}$" is logically equivalent to

$$(\exists u)(\exists w)\big(\langle u, v\rangle = \langle x, y\rangle \wedge \mathscr{F}(u, w)\big)$$

by III.8.7. By III.10.3 and the equivalence theorem, the above translates (is provably equivalent) to

$$(\exists u)(\exists w)\big(u = x \wedge v = y \wedge \mathscr{F}(u, w)\big)$$

Two applications of the one point rule yield the logically equivalent formula $\mathscr{F}(x, y)$.

With this settled, we see that ($ii$) and ($iii$) are indeed provably equivalent if $\mathbb{F}$ is given by ($i$).

(5) Since a function is a relation, all the notions and notation defined previously for relations apply to functions as well. We have some additional notation and concepts peculiar to functions: □

**III.11.14 Informal Definition.** If $\mathbb{F}$ is a function and $b \in \mathbb{F}\langle a\rangle$, then (by uniqueness of output) $\{b\} = \mathbb{F}\langle a\rangle$. *For functions only* we employ the abbreviation $b = \mathbb{F}(a)$. Note the round brackets.

If $a = \langle \vec{x}_n\rangle$ we agree to write $\mathbb{F}(\vec{x}_n)$ rather than $\mathbb{F}(\langle \vec{x}_n\rangle)$.

Functions that are sets will be generically denoted – unless they have specific names – by the letters $f, g, h$. □

[†] This informal definition gives the meaning of $z \in \{x : \mathscr{A}[x]\}$, *not* that of $z \in \{t[x] : \mathscr{A}[x]\}$.

We now see why we have two different notations for functions and relations when it comes to the image of an input. $\mathbb{F}(a)$ is the output itself, while $\mathbb{F}\langle a\rangle$ is the singleton $\{\mathbb{F}(a)\}$.[†]

**III.11.15 Example (Informal).** Here are two examples of relations from "real" mathematics: $C = \{\langle x, y\rangle \in \mathbb{R}^2 : x^2 + y^2 = 1\}$ and $H = \{\langle x, y\rangle \in \mathbb{R}^2 : x^2 + y^2 = 1 \wedge x \geq 0 \wedge y \geq 0\}$.

$H$, but not $C$, is a function. Clearly $H$ is the restriction of $C$ on the nonnegative reals, $\mathbb{R}_{\geq 0}$, in the sense $H = C \cap \mathbb{R}^2_{\geq 0}$. □

**III.11.16 Informal Definition (Function Substitution).** If $\mathbb{S}$ is a relation, $\mathscr{F}(x, y_1, \ldots, y_n)$ is a formula, and $\mathbb{G}$ is a function, then

$$\mathscr{F}(\mathbb{G}(x), y_1, \ldots, y_n) \quad \text{abbreviates} \quad (\exists z)(z = \mathbb{G}(x) \wedge \mathscr{F}(z, y_1, \ldots, y_n))$$

In particular, $\mathbb{G}(x)\,\mathbb{S}\,a$ stands for $(\exists z)(z = \mathbb{G}(x) \wedge z\,\mathbb{S}\,a)$, and $a\,\mathbb{S}\,\mathbb{G}(x)$ for $(\exists z)(z = \mathbb{G}(x) \wedge a\,\mathbb{S}\,z)$.

In short, we have introduced abbreviations that extend the one point rule in the informal domain, with informal terms such as $\mathbb{G}(x)$ that are not necessarily admissible in the formal theory. □

**III.11.17 Remark (Informal).** (1) Take the *relations* "=" ($\overset{\text{def}}{=} \{\langle x, y\rangle : x = y\}$) and "≠" ($\overset{\text{def}}{=} \{\langle x, y\rangle : \neg x = y\}$), both on $\mathbb{N}$, and a function $f : \mathbb{N} \to \mathbb{N}$. Then

$$y \neq f(x) \qquad \text{iff} \qquad (\exists z)(z \neq y \wedge z = f(x)) \qquad (i)$$

by III.11.16. Call this relation $F$. Also, let $T \overset{\text{def}}{=} \{\langle x, y\rangle : y = f(x)\}$.

Now $\mathbb{N}^2 - T = \{\langle x, y\rangle : f(x) \uparrow \vee (\exists z)(z \neq y \wedge z = f(x))\}$, for there are two ways to make $y = f(x)$ fail:

(a) $f(x) \uparrow$, since $y = f(x)$ implies $f(x) \downarrow$, or
(b) $(\exists z)(z \neq y \wedge z = f(x))$.

Thus, unless $f$ is *total* (in which case $f(x) \uparrow$ is false for all $x$), $\mathbb{N}^2 - T \neq F$.

This observation is very important if one works with nontotal functions a lot (e.g., in recursion theory).

[†] Sometimes one chooses to abuse notation and use "$\mathbb{F}(a)$" for both the singleton (thinking of $\mathbb{F}$ as a *relation*) and the "raw output" (thinking of $\mathbb{F}$ as a *function*). Of course the two uses of the notation are inconsistent, especially in the presence of foundation, and the context is being asked to do an unreasonable amount of fending against this. The $\mathbb{F}\langle x\rangle$ notation that we chose restores tranquillity.

(2) According to Definition III.11.16, for any functions $\mathbb{F}$ and $\mathbb{G}$, $\mathbb{F}(a) = \mathbb{G}(b)$ means $(\exists x)(\exists y)(x = \mathbb{F}(a) \wedge y = \mathbb{G}(b) \wedge x = y)$, or more simply, $(\exists x)(x = \mathbb{F}(a) \wedge x = \mathbb{G}(b))$. This is satisfactory for most purposes, but note that "$=$" between partial functions is not reflexive! Indeed, if both $\mathbb{F}(a)$ and $\mathbb{G}(b)$ are undefined, then they are not equal, although you would prefer them to be.

Kleene fixed this for the purposes of recursion theory with his *weak equality*, "$\simeq$", defined (informally) by

$$\mathbb{F}(a) \simeq \mathbb{G}(b) \quad \text{abbreviates} \quad \mathbb{F}(a)\uparrow \wedge\, \mathbb{G}(b)\uparrow \vee (\exists x)(x = \mathbb{F}(a) \wedge x = \mathbb{G}(b))$$

Clearly, $\vdash \mathbb{F}(a)\uparrow \wedge\, \mathbb{G}(b)\uparrow \rightarrow \mathbb{F}(a) \simeq \mathbb{G}(b)$.[†]

Whenever we use "$=$" we mean ordinary equality (where, in particular, $\mathbb{F}(a) = \mathbb{G}(b)$ entails $\mathbb{F}(a)\downarrow$ and $\mathbb{G}(b)\downarrow$). On those occasions where weak equality is employed, we will use the symbol "$\simeq$". □

**III.11.18 Exercise.** For any relations $\mathbb{S}$ and $\mathbb{T}$ prove

(1) $\mathbb{S} \subseteq \mathbb{T} \leftrightarrow (\forall x)(\mathbb{S}\langle x\rangle \subseteq \mathbb{T}\langle x\rangle)$,
(2) $\mathbb{S} = \mathbb{T} \leftrightarrow (\forall x)(\mathbb{S}\langle x\rangle = \mathbb{T}\langle x\rangle)$.

Also prove that for any two functions $\mathbb{F}$ and $\mathbb{G}$,

(3) $\mathbb{S} = \mathbb{T} \leftrightarrow (\forall x)(\mathbb{S}(x) \simeq \mathbb{T}(x))$

while

(4) $\mathbb{S} = \mathbb{T} \leftrightarrow (\forall x)(\mathbb{S}(x) = \mathbb{T}(x))$ fails. □

**III.11.19 Exercise.** For any (formal) term $t(\vec{x}_n)$ and class term $\mathbb{A}$, the class term

$$\mathbb{F} = \{\langle \vec{x}_n, t(\vec{x}_n)\rangle : \langle \vec{x}_n\rangle \in \mathbb{A}\}$$

is the binary relation (see III.8.7)

$$\mathbb{F} = \Big\{z : OP(z) \wedge (\exists x_1)\ldots(\exists x_n)\Big(\pi(z) = \langle \vec{x}_n\rangle \wedge \delta(z) = t(\vec{x}_n) \wedge \pi(z) \in \mathbb{A}\Big)\Big\}$$

Prove that $\mathbb{F}$ is single-valued in the second projection ($\delta(z)$), and hence is a function. □

**III.11.20 Informal Definition ($\lambda$-Notation).** We use a variety of notations to indicate the dependence of the function $\mathbb{F}$ of the preceding exercise on the "defining term" $t$, usually letting $\mathbb{A}$ be understood from the context. We may

[†] Indeed not just "$\vdash$", but "$\models_{\mathbf{Taut}}$". On the right hand side of "$\rightarrow$" we expand the abbreviation into $\mathbb{F}(a)\uparrow \wedge\, \mathbb{G}(b)\uparrow \vee (\exists x)(x = \mathbb{F}(a) \wedge x = \mathbb{G}(b))$.

write any of the following:

(1) $\mathbb{F}(\vec{x}_n) = t(x_1, \ldots, x_n)$ for all $\vec{x}_n$ (recall that we write $\mathbb{F}(\vec{x}_n)$ rather than $\mathbb{F}(\langle\vec{x}_n\rangle)$ and that $\langle\vec{x}_n, y\rangle = \langle\langle\vec{x}_n\rangle, y\rangle$).
(2) $\mathbb{F} = \big(\vec{x}_n \mapsto t(x_1, \ldots, x_n)\big)$.
(3) $\mathbb{F} = \lambda\vec{x}_n.t(x_1, \ldots, x_n)$ ($\lambda$-notation). □

**III.11.21 Example (Informal).** If we work in $\mathbb{N}$ informally, we can define – from the term $y^2$ – a function

$$f = \{\langle\langle x, y\rangle, y^2\rangle : \langle x, y\rangle \in \mathbb{N}^2\} \tag{1}$$

We can then write

$$f = \lambda xy.y^2 \tag{2}$$

This function has two inputs. One, $x$, is ignored when the output is "computed". Such variables (inputs) are sometimes called "dummy variables".

$\lambda$-notation gives us the list of variables (between $\lambda$ and ".") and the "rule" for finding the output (after the "."). The left and right fields (here $\mathbb{N}^2$ and $\mathbb{N}$ respectively) must by understood from the context.

In practice one omits the largely ceremonial part of introducing (1) and writes (2) at once. □

Some restricted types of functions are important.

**III.11.22 Informal Definition.** A function $\mathbb{F}$ is *one-to-one*, or simply 1-1, iff it is single-valued in the first projection, that is,

$$z \in \mathbb{F} \wedge w \in \mathbb{F} \wedge \delta(z) = \delta(w) \rightarrow \pi(z) = \pi(w) \tag{1}$$

Alternatively, we may write

$$\mathbb{F}(x) = \mathbb{F}(y) \rightarrow x = y \tag{2}$$

A 1-1 function is also called *injective* or an *injection*. □

As we feel obliged after the introduction of new *argot* to issue the usual clarifications, we state: When used in ZFC, "$\mathbb{F}$ is 1-1" is just short for (1) or (2) above. Thus, to *assume* that $\mathbb{F}$ is 1-1 is tantamount to adding (1) (equivalently, (2)) to the axioms, while to *claim* that $\mathbb{F}$ is 1-1 is the same as asserting its (ZFC) provability.

Note that $\mathbb{F}(x) = \mathbb{F}(y)$ implies that both sides of "=" are defined (cf. III.11.16). In the opposite situation $\mathbb{F}(x) = \mathbb{F}(y)$ is refutable; hence (2) still holds.

The above definition can also be stated as $u\ \mathbb{F}\ x \wedge u\ \mathbb{F}\ y \rightarrow x = y$. We can say that a 1-1 function "distinguishes inputs", in that distinct inputs *of its domain* are mapped into distinct outputs.

Note that $f = \{\langle 0, 1\rangle, \langle 1, 2\rangle\}$ is 1-1 by III.11.22, but while $f(2) \simeq f(3)$ (III.11.17), it is the case that $2 \neq 3$. Nevertheless, $f(2) = f(3) \rightarrow 2 = 3$, since $f(2) = f(3)$ is refutable.

*1-1-ness* is a notion that is independent of left or right fields (unlike the notions *total*, *nontotal*, *onto*).

**III.11.23 Example.** A function $\mathbb{F}$ is 1-1 iff $\mathbb{F}^{-1}$ is a function. Indeed, $\mathbb{F}$ is 1-1 iff it is single-valued in the first projection, iff $\mathbb{F}^{-1}$ is single-valued in the second projection. □

**III.11.24 Informal Definition (1-1 correspondences).** A function $\mathbb{F} : \mathbb{A} \rightarrow \mathbb{B}$ is a *1-1 correspondence* iff it is 1-1, total, and onto. We say that $\mathbb{A}$ and $\mathbb{B}$ are *in 1-1 correspondence* and write

$$\mathbb{A} \sim \mathbb{B} \qquad \text{or} \qquad \mathbb{A} \overset{\mathbb{F}}{\sim} \mathbb{B}$$

□

A 1-1 correspondence is also called a *bijection*, or a *bijective* function. An onto function is also called a *surjection*, or *surjective*.

**III.11.25 Example (Informal).** The notion of 1-1 correspondence is very important. If two sets are in 1-1 correspondence, then, intuitively, they have "the same number of elements". On this observation rests the theory of cardinality and cardinal numbers (Chapter VII).

For example, $\lambda n.2n : \mathbb{N} \rightarrow \{2n : n \in \mathbb{N}\}$ is a 1-1 correspondence between all natural numbers and all even (natural) numbers. □

Let us now re-formulate the axiom of collection with the benefit of relational and functional notation.

**III.11.26 Theorem (Collection in *Argot*).**

(1) *For any relation* $\mathbb{S}$ *such that* $\mathrm{dom}(\mathbb{S})$ *is a* set, *there is a set* $B$ *such that* $\mathbb{S}^{-1}[B] = \mathrm{dom}(\mathbb{S})$.

(2) *For any relation* $\mathbb{S}$ *such that* $\mathrm{ran}(\mathbb{S})$ *is a* set, *there is a set* $A$ *such that* $\mathbb{S}[A] = \mathrm{ran}(\mathbb{S})$.

*Proof.* (1): Let $\mathbb{S} = \{\langle x, y\rangle : \mathscr{S}(x, y)\}$ for some formula $\mathscr{S}$ of the formal language. Let $Z = \mathrm{dom}(\mathbb{S})$. An instance of "verbose" collection (cf. III.8.4) is

$$(\forall x \in Z)(\exists y)\mathscr{S}(x, y) \to (\exists W)\big(\neg U(W) \wedge (\forall x \in Z)(\exists y \in W)\mathscr{S}(x, y)\big) \quad (i)$$

Now, we are told that $Coll_x(\exists y)\mathscr{S}(x, y)$ (cf. III.11.4); thus the assumption $Z = \mathrm{dom}(\mathbb{S})$ translates into

$$\vdash_{\mathrm{ZFC}} (\forall x)\big(x \in Z \leftrightarrow (\exists y)\mathscr{S}(x, y)\big)$$

and therefore the left hand side of $(i)$ is provable, by tautological implication and $\forall$-monotonicity (I.4.24). Thus the following is also a theorem:

$$(\exists W)\big(\neg U(W) \wedge (\forall x \in Z)(\exists y \in W)\mathscr{S}(x, y)\big) \qquad (ii)$$

Let us translate $(ii)$ into *argot*: We are told that a set $W$ exists[†] such that

$$(\forall x \in Z)(\exists y)(y \in W \wedge y \in \mathbb{S}\langle x\rangle)$$

Hence

$$(\forall x \in Z) W \cap \mathbb{S}\langle x\rangle \neq \emptyset$$

and finally (see Remark III.11.5(5))

$$Z \subseteq \mathbb{S}^{-1}[W]$$

Since, trivially, $Z \supseteq \mathbb{S}^{-1}[W]$ we see that $W$ will do for the sought $B$.

(2) follows from (1) using $\mathbb{S}^{-1}$ instead of $\mathbb{S}$. □

**III.11.27 Remark.** Statement (1) in the theorem, and therefore (2), are "equivalent" to collection. That is, if we have (1), then we also have $(i)$ above. To see this, let $\mathscr{S}(x, y)$ of the formal language satisfy the hypothesis of collection, $(i)$:

$$(\forall x \in Z)(\exists y)\mathscr{S}(x, y) \qquad (a)$$

for some set $Z$. Let us define $\mathbb{S} \overset{\mathrm{def}}{=} \{\langle x, y\rangle : \mathscr{S}(x, y) \wedge x \in Z\}$. Then $(a)$ yields $Z = \mathrm{dom}(\mathbb{S})$. (1) now implies that for some set $B$, $Z \subseteq \mathbb{S}^{-1}[B]$, from which the reader will have no trouble deducing

$$(\forall x \in Z)(\exists y \in B)\mathscr{S}(x, y) \qquad (b)$$

$(b)$ proves $(\exists W)\big(\neg U(W) \wedge (\forall x \in Z)(\exists y \in W)\mathscr{S}(x, y)\big)$. □

[†] We are using the auxiliary constant $W$, in other words.

**III.11.28 Proposition.**

(1) *If* $\mathbb{S}$ *is a function and* $A$ *is a set, then so is* $\mathbb{S}[A]$.
(2) *If* $\mathbb{S}$ *is a function and* $\mathrm{dom}(\mathbb{S})$ *is a set, then so is* $\mathrm{ran}(\mathbb{S})$.

*Proof.* (2) follows from (1), since $\mathrm{ran}(\mathbb{S}) = \mathbb{S}[\mathrm{dom}(\mathbb{S})]$.

As for (1), it is *argot* for collection version III.8.12(4). Indeed, letting

$$\mathbb{S} = \{\langle x, y\rangle : \mathscr{S}(x, y)\}$$

the assumption that $\mathbb{S}$ is a function yields (cf. III.11.13(4)) the theorem

$$\mathscr{S}(x, y) \wedge \mathscr{S}(x, z) \to y = z$$

The aforementioned version of collection then yields

$$Coll_y(\exists x \in A)\mathscr{S}(x, y)$$

i.e., that the class term

$$\{y : (\exists x \in A)\mathscr{S}(x, y)\}$$

can be formally introduced (“is a set”). This is exactly what we want. □

☡☡ We have already noted in III.8.3(II), p. 164, that the proposition – being an *argot* rendering of III.8.12(4) – is equivalent to collection III.8.2.[†] A proof of this equivalence will be given later once *rank* (of set) and *stage* (of set construction) have been defined rigorously. In the meanwhile, in practice, the proposition (i.e., collection version III.8.12(4)) will often be used in lieu of collection (being an implication of the latter, this is legitimate). ☡☡

**III.11.29 Corollary.** *If* $\mathbb{F}$ *is a function and* $\mathrm{dom}(\mathbb{F})$ *is a set, then* $\mathbb{F}$ *is a set.*

*Proof.* By III.11.28, $\mathrm{ran}(\mathbb{F})$ is a set. But $\mathbb{F} \subseteq \mathrm{dom}(\mathbb{F}) \times \mathrm{ran}(\mathbb{F})$.

Alternatively, let $\mathbb{G} \overset{\mathrm{def}}{=} \{\langle x, \langle x, \mathbb{F}(x)\rangle\rangle : x \in \mathrm{dom}(\mathbb{F})\}$. Clearly, $\mathbb{G}$ is a function and $\mathrm{dom}(\mathbb{G}) = \mathrm{dom}(\mathbb{F})$, while $\mathrm{ran}(\mathbb{G}) = \mathbb{F}$. □

The notion of function allows us to see families of sets from a slightly different notational viewpoint. More importantly, it allows us to extend the notion of Cartesian product. First of all,

**III.11.30 Informal Definition (Indexed Families of Sets).** A function $\mathbb{F}$ such that $\mathrm{ran}(\mathbb{F})$ contains no urelements is an *indexed family of sets*. $\mathrm{dom}(\mathbb{F})$ is the *index class*. If $\mathrm{dom}(\mathbb{F}) = \emptyset$, then we have an *empty* indexed family.

[†] Or, as we simply say, collection.

If we let $\mathbb{I}$ be a name for dom($\mathbb{F}$), then we often write $(\mathbb{F}_a)_{a\in\mathbb{I}}$ to denote the indexed family, rather than just $\mathbb{F}$ or $\lambda a.\mathbb{F}(a)$.

In the notation "$\mathbb{F}_a$" it is *not* implied that $\mathbb{F}(a)$ might be a proper class (it cannot be); rather we imply that the *function* $\mathbb{F}$ might be a proper class. □

Note that we called $\mathbb{F}$, rather than ran($\mathbb{F}$), the indexed family (of course, ran($\mathbb{F}$) is a family of sets in the sense of III.6.3, p. 150). What is new here is the intention to allow "multiple copies" of a set in a family with the help of $\mathbb{F}$. An *indexed* family allows us to be able to talk about, say, $S = \{a, b, a, a, c, d\}$ without being obliged to collapse the multiple $a$-elements into one (extensionality would dictate this if we had just a set or class $\{a, b, a, a, c, d\}$). This freedom is achieved by thinking of the first $a$ as, say, $f(0)$, the second as $f(2)$, and the third as $f(3)$, where

$$f = \{\langle 0, a\rangle, \langle 1, b\rangle, \langle 2, a\rangle, \langle 3, a\rangle, \langle 4, c\rangle, \langle 5, d\rangle\}$$

is an indexed family with index set $\mathrm{dom}(f) = \{0, 1, 2, 3, 4, 5\}$, and $\mathrm{ran}(f) = S$. Why is this useful?

For example, if $a, b, c, d, \ldots$ are cardinals (Chapter VII), we may want to study sums of these where multiple summands may be equal to each other. We can achieve this with a concept/notation like $\sum_{i\in\mathrm{dom}(f)} f(i)$.

This situation is entirely analogous to one that occurs in the study of series in real analysis, where repeated terms are also allowed.

**III.11.31 Example.** Every family of sets $\mathbb{A}$ in the sense of III.6.3 leads to an *indexed* family of sets $\lambda x.x$ that has $\mathbb{A}$ as domain or index class.

Here is a family of sets in informal mathematics: $\{(0, 1/n) : n \in \mathbb{N} - \{0\}\}$, where "$(a, b)$" here stands for *open interval* of real numbers. This can be viewed as an indexed family fitting the general scheme – $\lambda x.x$ – above.

A more natural way is to view it as the indexed family $\lambda n.(0, 1/n)$ of domain $\mathbb{N} - \{0\}$, that is, $\big((0, 1/n)\big)_{n\in\mathbb{N}-\{0\}}$. □

**III.11.32 Informal Definition.** Let $(\mathbb{F}_a)_{a\in\mathbb{I}}$ be an indexed family of sets. Then

$$\bigcup_{a\in\mathbb{I}} \mathbb{F}_a \stackrel{\text{def}}{=} \bigcup \mathrm{ran}(\mathbb{F})$$

$$\bigcap_{a\in\mathbb{I}} \mathbb{F}_a \stackrel{\text{def}}{=} \bigcap \mathrm{ran}(\mathbb{F})$$

If $\mathbb{I}$ is a set $I$, then

$$\prod_{a\in I} \mathbb{F}_a \stackrel{\text{def}}{=} \{f : f \text{ is a function } \wedge \mathrm{dom}(f) = I \wedge (\forall a \in I) f(a) \in \mathbb{F}_a\}$$

If, for each $a \in I$, $\mathbb{F}_a = A$, the same set, then $\prod_{a\in I} \mathbb{F}_a$ is denoted by ${}^I A$. That is, ${}^I A$ is the class of all *total* functions from $I$ to $A$:

$$\{f : f \text{ is a function } \wedge \operatorname{dom}(f) = I \wedge (\forall a \in I) f(a) \in A\} \qquad \square$$

**III.11.33 Remark.** (1) $\bigcup_{a\in\mathbb{I}} \mathbb{F}_a$ and $\bigcap_{a\in\mathbb{I}} \mathbb{F}_a$ just introduce new notation (see also the related III.10.22, p. 192). However, $\prod_{a\in I} \mathbb{F}_a$ is a new concept that is related but is not identical to the "finite" Cartesian product. For example, if $A_1 = \{1\}$ and $A_2 = \{2\}$, then

$$\bigtimes_{i=1}^{2} A_i = A_1 \times A_2 = \{\langle 1, 2\rangle\} \qquad (i)$$

while if we consider the indexed family $(A_i)_{i\in\{1,2\}}$, then

$$\prod_{i\in\{1,2\}} A_i = \big\{\{\langle 1, 1\rangle, \langle 2, 2\rangle\}\big\} \qquad (ii)$$

In general, an element of $A_1 \times \cdots \times A_n$ is an $n$-vector $\langle x_1, \ldots, x_n\rangle$, while an element of $\prod_{i\in\{1,\ldots,n\}} A_i$ is a *sequence* $f = \{\langle 1, x_1\rangle, \ldots, \langle n, x_n\rangle\}$. Sequences are not tuples, but they do give, in a different way, *positional information*, just as tuples do. Sequences have the additional flexibility of being able to have "infinite" length (intuitively). Thus, while $\langle a_1, a_2, \ldots\rangle$, where "..." stands for $a_i$ for all $i \in \mathbb{N}$, is meaningless as a tuple, it can be captured as a sequence $f$, where $\operatorname{dom}(f) = \mathbb{N}$ and $f(i) = a_i$ for all $i \in \mathbb{N}$. This makes sequences preferable to vectors in practice.

In this discussion we are conversing within informal (meta)mathematics. We must not forget that in the formal theory we mirror only those objects that we have proved to *exist* so far – i.e., to have counterparts, or representations, *within the theory*; the arbitrary $n$, and $\mathbb{N}$, are not among them.

(2) Requiring $\mathbb{I}$ to be a set in the definition of $\prod$ ensures that the functions $f$ that we collect into $\prod$ are sets (by III.11.29). This is necessary, for classes can only have elements that are sets or atoms.

(3) The sub-formula "$f$ is a function" is *argot* for

$$(\forall z \in f)\Big(OP(z) \wedge (\forall w \in f)\big(\pi(z) = \pi(w) \rightarrow \delta(z) = \delta(w)\big)\Big) \qquad \square$$

**III.11.34 Proposition.** *If $I$ is a set, then $\bigcup_{a\in I} \mathbb{F}_a$ and $\prod_{a\in I} \mathbb{F}_a$ are sets. If moreover $I \neq \emptyset$, then $\bigcap_{a\in I} \mathbb{F}_a$ is a set as well.*

*Proof.* Since $I$ is a set, so is $\mathrm{ran}(\mathbb{F})$ by III.11.28. Now the cases for $\bigcup_{a\in I}\mathbb{F}_a$ and $\bigcap_{a\in I}\mathbb{F}_a$ follow from III.11.32 and the axiom of union and from III.6.14, respectively.

On the other hand,

$$\prod_{a\in I}\mathbb{F}_a \subseteq \mathbf{P}(I \times \bigcup_{a\in I}\mathbb{F}_a)$$

Hence $\prod_{a\in I}\mathbb{F}_a$ is a set. □

**III.11.35 Corollary.** *For any sets $A$ and $B$, ${}^{A}B$ is a set.*

**III.11.36 Example.** Let $A, B, C$ be nonempty sets, that is, suppose we have proved

$$(\exists x)x \in A$$

$$(\exists x)x \in B$$

and

$$(\exists x)x \in C$$

Let (by auxiliary constant)

$$a \in A$$

$$b \in B$$

$$c \in C$$

Then $\langle a, b, c\rangle \in A \times B \times C$; hence we have proved in ZFC

$$(\exists x)x \in A \wedge (\exists x)x \in B \wedge (\exists x)x \in C \rightarrow (\exists x)x \in A \times B \times C$$

We can do the same with four sets, or five sets, or eleven sets, etc., or prove by (informal) induction on $n$, *in the metatheory*, the *theorem schema* (see III.10.21)

$$\text{if} \quad A_i \neq \emptyset \text{ for } i = 1, \ldots, n, \quad \text{then} \quad \bigtimes_{1\le i\le n} A_i \neq \emptyset. \tag{1}$$

Metatheoretically speaking, we can "implement" any $n$-tuple $\langle \vec{a}_n\rangle \in \bigtimes_{1\le i\le n} A_i$ as a *sequence* $f = \{\langle i, a_i\rangle : 1 \le i \le n\}$. That is, the function $f$ is a set (by III.11.29) applied to the (informal) set $I = \{1, 2, 3, \ldots, n\}$.[†] Thus, $f \in \prod_{i\in I} A_i$.

[†] Thinking of the informal natural numbers as urelements, $I$ is a set by separation, since the "real" $M$ is a set.

It follows that

$$\text{if} \quad A_i \neq \emptyset \text{ for } i = 1, \ldots, n, \quad \text{then} \quad \prod_{i \in I} A_i \neq \emptyset. \tag{2}$$

(2) can be obtained *within* the theory, once $n$ and $\mathbb{N}$ are formalized. In the meanwhile, we can view it, *formally*, not as *one* statement, but as a compact way of representing infinitely many statements (a theorem schema): One with one set $A$ (called $A_1$ in (2)), one with two sets $A, B$ ($A_1, A_2$), one with three sets $A, B, C$ ($A_1, A_2, A_3$), etc.

As indices we can use, for example, $\{\emptyset\}$, $\{\{\emptyset\}\}$, $\{\{\{\emptyset\}\}\}$, $\{\{\{\{\emptyset\}\}\}\}$, etc., which are all distinct (why?).[†]

Does (2) extend to the case of arbitrary (and therefore possibly infinite) $I$? We consider this question in the next chapter. □

We have seen the majority of nonlogical axioms for ZFC in this chapter. The "C" of ZFC is considered in the next chapter. In Chapter V we will introduce the last axiom, the *axiom of infinity*, which implies that infinite sets exist.[‡]

### III.12. Exercises

**III.1.** Prove $\vdash_{\mathrm{ZFC}} \neg U(A) \wedge \neg U(B) \rightarrow (A \subset B \rightarrow B \neq \emptyset)$.

**III.2.** Prove $\vdash_{\mathrm{ZFC}} Coll_x \mathscr{B} \rightarrow (\forall x)(\mathscr{A} \rightarrow \mathscr{B}) \rightarrow Coll_x \mathscr{A}$.

**III.3.** Prove $\vdash_{\mathrm{ZFC}} U(x) \rightarrow x \cap y = \emptyset$.

**III.4.** Prove $\vdash_{\mathrm{ZFC}} U(x) \rightarrow x - y = \emptyset$.

**III.5.** Prove $\vdash_{\mathrm{ZFC}} \neg U(x) \rightarrow U(y) \rightarrow x - y = x$.

**III.6.** Let $a$ be a set, and consider the class $b = \{x \in a : x \notin x\}$. Show that, despite similarities with the Russell class $R$, $b$ *is* a set. Moreover, show $\vdash b \notin a$. Do *not* use foundation.

**III.7.** Show $\vdash$ $R$ (the Russell class) $= \mathbb{U}_M$.

**III.8.** Show that $\vdash_{\mathrm{ZFC}} \neg U(x) \rightarrow \emptyset \subseteq x$

**III.9.** Show that if a class $\mathbb{A}$ satisfies $\mathbb{A} \subseteq x$ for all sets $x$, then $\mathbb{A} = \emptyset$.

**III.10.** Without using foundation, show that $\emptyset \neq \{\emptyset\}$.

[†] We can still *write* these indices as "1", "2", "3", "4", etc. (essentially counting the nesting of {}-brackets), as this is more pleasing visually.

[‡] The infinity axiom does not just say that infinite sets exist. It says, essentially, that limit ordinals exist, which is a stronger assertion.

**III.11.** Interpret the extensionality axiom over $\mathbb{N}$ so that the variables vary over integers, not sets, and $\in$ is interpreted as "less than", $<$. Show that under this interpretation the axiom is true.

**III.12.** Show that if we have no urelements, and if our axioms are just extensionality, separation, union, foundation, and collection, then this set theory

(1) can prove that a set exists, but

(2) cannot prove that a nonempty set exists.

$\big($*Hint*: Find a model of all the above axioms augmented by the formula $(\forall y)\big(\neg U(y) \to (\forall x)x \notin y\big)$.$\big)$

**III.13.** Suppose we have all the axioms except the one for pairing and the one that asserts the existence of a set of urelements (III.3.1). Show that these axioms cannot prove that a set exists.

(*Hint*: Find a model of all the above axioms augmented by the formula $(\forall x)U(x)$.)

**III.14.** (Bourbaki (1966b)) Drop collection version III.8.2, separation, and union. Add Bourbaki's axiom of "selection and union", that is, collection version (2) of III.8.12, p. 173. Prove that separation and union are now theorems.

**III.15.** (Shoenfield (1967)) Drop collection version III.8.2, pairing, and union. Add collection version (3) of III.8.12, p. 173. Prove that pairing and union are now theorems.

**III.16.** (Levy (1979)) Drop collection version III.8.2, pairing, and separation. Add collection version (4) of III.8.12, p. 173. Prove that pairing and separation are now theorems.

**III.17.** Prove

$$U(A) \to \mathbf{P}(A) = \{\emptyset\}$$

in ZFC.

**III.18.** What is $\bigcap \emptyset$ (and why)?

**III.19.** Show that

(1) $\vdash \mathbb{A} \cup \mathbb{B} = \mathbb{B} \cup \mathbb{A}$ and

(2) $\vdash \mathbb{A} \cup (\mathbb{B} \cup \mathbb{C}) = (\mathbb{A} \cup \mathbb{B}) \cup \mathbb{C}$.

**III.20.** Show that

(1) $\vdash \mathbb{A} \cap \mathbb{B} = \mathbb{B} \cap \mathbb{A}$ and

(2) $\vdash \mathbb{A} \cap (\mathbb{B} \cap \mathbb{C}) = (\mathbb{A} \cap \mathbb{B}) \cap \mathbb{C}$.

**III.21.** For any set $A$ in the "restricted" universe $\mathbb{U}_N$ ($N \subseteq M$), show that $\mathbb{U}_N - A$ is a proper class.

**III.22.** Show for any classes $\mathbb{A}, \mathbb{B}$ that $\mathbb{A} - \mathbb{B} = \mathbb{A} - \mathbb{A} \cap \mathbb{B}$.

**III.23.** For any classes $\mathbb{A}, \mathbb{B}$ show that $\mathbb{A} \cup \mathbb{B} = \mathbb{A}$ iff $\mathbb{B} \subseteq \mathbb{A}$.

**III.24.** For any classes $\mathbb{A}, \mathbb{B}$ show that $\mathbb{A} \cap \mathbb{B} = \mathbb{A}$ iff $\mathbb{A} \subseteq \mathbb{B}$.

**III.25.** For any classes $\mathbb{A}, \mathbb{B}$ show that $\mathbb{A} - (\mathbb{A} - \mathbb{B}) = \mathbb{B}$ iff $\mathbb{B} \subseteq \mathbb{A}$.

**III.26.** Prove III.6.15(2).

**III.27.** (1) Express $\mathbb{A} \cap \mathbb{B}$ using class difference as the only operation.
(2) Express $\mathbb{A} \cup \mathbb{B}$ using class difference and complement as the only operations.

**III.28.** *Generalized De Morgan's laws*. Prove for any class $\mathbb{A}$ and indexed family $(\mathbb{B}_i)_{i \in \mathbb{F}}$ that

$$\mathbb{A} - \bigcup_{i \in \mathbb{F}} \mathbb{B}_i = \bigcap_{i \in \mathbb{F}} (\mathbb{A} - \mathbb{B}_i) \tag{1}$$

$$\mathbb{A} - \bigcap_{i \in \mathbb{F}} \mathbb{B}_i = \bigcup_{i \in \mathbb{F}} (\mathbb{A} - \mathbb{B}_i) \tag{2}$$

**III.29.** *Distributive laws for* $\cup, \cap$. For any classes $\mathbb{A}, \mathbb{B}, \mathbb{D}$ show

$$\mathbb{A} \cap (\mathbb{B} \cup \mathbb{D}) = (\mathbb{A} \cap \mathbb{B}) \cup (\mathbb{A} \cap \mathbb{D}) \tag{1}$$

$$\mathbb{A} \cup (\mathbb{B} \cap \mathbb{D}) = (\mathbb{A} \cup \mathbb{B}) \cap (\mathbb{A} \cup \mathbb{D}) \tag{2}$$

**III.30.** *Generalized distributive laws for* $\cup, \cap$. Prove for any class $\mathbb{A}$ and indexed family $(\mathbb{B}_i)_{i \in \mathbb{F}}$ that

$$\mathbb{A} \cap \bigcup_{i \in \mathbb{F}} \mathbb{B}_i = \bigcup_{i \in \mathbb{F}} (\mathbb{A} \cap \mathbb{B}_i) \tag{1}$$

$$\mathbb{A} \cup \bigcap_{i \in \mathbb{F}} \mathbb{B}_i = \bigcap_{i \in \mathbb{F}} (\mathbb{A} \cup \mathbb{B}_i) \tag{2}$$

**III.31.** Show that we cannot have $a \in b \in c \in \cdots \in a$.

**III.32.** Show that $\mathbb{V}_N$ is a proper class for any set $N$ of urelements (including the case $N = \emptyset$).

**III.33.** Show that for any class (not just set) $\mathbb{A}$, $\mathbb{A} \in \mathbb{A}$ is refutable.

**III.34.** (1) Show that $\mathbb{A} =$"the class of *all* sets that contain at least one element" can be defined by a class term.
(2) Show that $\mathbb{A}$ is a proper class.

**III.35.** Attach the *intuitive meaning* to the statement that the set $A$ has $n$ distinct elements. Show then, by informal induction on $n \in \mathbb{N}$, that for $n \geq 0$, if $A$ has $n$ elements, then $\mathbf{P}(A)$ has $2^n$ elements.

**III.36.** Show (without the use of foundation) that $\big\{\{a\}, \{a, b\}\big\} = \big\{\{a'\}, \{a', b'\}\big\}$ implies $a = a'$ and $b = b'$.

**III.37.** For any sets $x$, $y$ show that $x \cup \{x\} = y \cup \{y\} \to x = y$.
(*Hint*: Use foundation.)

**III.38.** Prove Proposition III.10.13.

**III.39.** Prove Proposition III.10.14.

**III.40.** For any $\mathbb{A}, \mathbb{B}$ show that $\emptyset = \mathbb{A} \times \mathbb{B}$ iff $\mathbb{A} = \emptyset$ or $\mathbb{B} = \emptyset$.

**III.41.** For any set of urelements $N$, show that $\mathbb{U}_N^3 \subseteq \mathbb{U}_N^2$.

**III.42.** *Distributive law for* ×. Show for any $\mathbb{A}$, $\mathbb{B}$ and $\mathbb{D}$ that $\mathbb{D} \times (\mathbb{A} \cup \mathbb{B}) = (\mathbb{D} \times \mathbb{A}) \cup (\mathbb{D} \times \mathbb{B})$.

**III.43.** Let $\mathbb{F} : \mathbb{X} \to \mathbb{Y}$ be a function, and $\mathbb{A} \subseteq \mathbb{Y}$, $\mathbb{B} \subseteq \mathbb{Y}$. Prove
(a) $\mathbb{F}^{-1}[\mathbb{A} \cup \mathbb{B}] = \mathbb{F}^{-1}[\mathbb{A}] \cup \mathbb{F}^{-1}[\mathbb{B}]$
(b) $\mathbb{F}^{-1}[\mathbb{A} \cap \mathbb{B}] = \mathbb{F}^{-1}[\mathbb{A}] \cap \mathbb{F}^{-1}[\mathbb{B}]$
(c) if $\mathbb{A} \subseteq \mathbb{B}$, then $\mathbb{F}^{-1}[\mathbb{B} - \mathbb{A}] = \mathbb{F}^{-1}[\mathbb{B}] - \mathbb{F}^{-1}[\mathbb{A}]$.
Is this last equality true if $\mathbb{A} \not\subseteq \mathbb{B}$? Why?

**III.44.** Let $\mathbb{F} : \mathbb{X} \to \mathbb{Y}$ be a function, and $\mathbb{A} \subseteq \mathbb{X}$, $\mathbb{B} \subseteq \mathbb{X}$. Prove
(a) $\mathbb{F}[\mathbb{A} \cup \mathbb{B}] = \mathbb{F}[\mathbb{A}] \cup \mathbb{F}[\mathbb{B}]$
(b) $\mathbb{F}[\mathbb{A} \cap \mathbb{B}] \subseteq \mathbb{F}[\mathbb{A}] \cap \mathbb{F}[\mathbb{B}]$
(c) if $\mathbb{A} \subseteq \mathbb{B}$, then $\mathbb{F}[\mathbb{B} - \mathbb{A}] \supseteq \mathbb{F}[\mathbb{B}] - \mathbb{F}[\mathbb{A}]$.
Can the above inclusions be sharpened to equalities? Why?

**III.45.** Which parts, if any, of the above two problems generalize to the case that $\mathbb{F}$ is just a relation?

**III.46.** Let $\mathbb{G}$ be a function and $\mathbb{F}$ a family of sets. Prove
(a) $\mathbb{G}^{-1}\big[\bigcup \mathbb{F}\big] = \bigcup \mathbb{G}^{-1}\big[\mathbb{F}\big]$
(b) $\mathbb{G}^{-1}\big[\bigcap \mathbb{F}\big] = \bigcap \mathbb{G}^{-1}\big[\mathbb{F}\big]$
(c) $\mathbb{G}\big[\bigcup \mathbb{F}\big] = \bigcup \mathbb{G}\big[\mathbb{F}\big]$
(d) $\mathbb{G}\big[\bigcap \mathbb{F}\big] \subseteq \bigcap \mathbb{G}\big[\mathbb{F}\big]$. (Can $\subseteq$ be replaced by $=$? Why?)

**III.47.** Let $\mathbb{F}$ be a function, and $\mathbb{A}$ a class. Prove
(a) $\mathbb{F}[\mathbb{F}^{-1}[\mathbb{A}]] \subseteq \mathbb{A}$
(b) $\mathbb{F}^{-1}[\mathbb{F}[\mathbb{A}]] \supseteq \mathbb{A}$, provided that $\mathbb{A} \subseteq \mathrm{dom}(\mathbb{F})$.
Show by appropriate concrete examples that the above inclusions cannot be sharpened, in general, to equalities.

**III.48.** Let the function $\mathbb{F}$ be 1-1, while $\mathbb{A} \subseteq \mathrm{dom}(\mathbb{F})$ is an arbitrary class. Show that $\mathbb{F}^{-1}[\mathbb{F}[\mathbb{A}]] = \mathbb{A}$. State and prove an appropriate converse.

**III.49.** Let $\mathbb{B} \subseteq \mathrm{ran}(\mathbb{G})$. Prove $\mathbb{G}[\mathbb{G}^{-1}[\mathbb{B}]] = \mathbb{B}$. State and prove an appropriate converse.

**III.50.** Let $\mathbb{F}$ be a 1-1 function and $\mathbb{A} \subseteq \mathbb{B} \subseteq \mathrm{dom}(\mathbb{F})$.

(a) Prove $\mathbb{F}[\mathbb{B} - \mathbb{A}] = \mathbb{F}[\mathbb{B}] - \mathbb{F}[\mathbb{A}]$.

(b) Prove a suitable converse.

Is the restriction $\mathbb{A} \subseteq \mathbb{B} \subseteq \mathrm{dom}(\mathbb{F})$ necessary? Why?

**III.51.** For any relations $\mathbb{S}$, $\mathbb{T}$ prove

(1) $(\mathbb{S}^{-1})^{-1} = \mathbb{S}$

(2) $\mathrm{dom}(\mathbb{S}) = \mathrm{ran}(\mathbb{S}^{-1})$

(3) $\mathrm{ran}(\mathbb{S}) = \mathrm{dom}(\mathbb{S}^{-1})$

(4) $(\mathbb{S} \cup \mathbb{T})^{-1} = \mathbb{S}^{-1} \cup \mathbb{T}^{-1}$.

**III.52.** Prove that if $(\mathbb{S}^{-1})^{-1} = \mathbb{S}$, then $\mathbb{S}$ is a relation. Give an example where the equality fails. Which ones among (2)–(4) in the previous exercise hold for arbitrary classes?

**III.53.** Using only the axioms of union, pairing, and separation, show that if a function $\mathbb{F}$ is a set, then so are both $\mathrm{dom}(\mathbb{F})$ and $\mathrm{ran}(\mathbb{F})$.

**III.54.** Show for a relation $\mathbb{S}$ that if both the range and the domain are sets, then $\mathbb{S}$ is a set.

**III.55.** Show that if a relation $S$ is a set, then so is $S^{-1}$.

**III.56.** If $\mathbb{F} : \mathbb{A} \to \mathbb{B}$ is a 1-1 correspondence, show that so is $\mathbb{F}^{-1} : \mathbb{B} \to \mathbb{A}$.

# IV

# The Axiom of Choice

From this chapter and onwards the reader will witness more and more the "relaxed proof style" (cf. III.5.9).

## IV.1. Introduction

The previous chapter concluded with the question, can

$$\text{if} \quad A_i \neq \emptyset \text{ for all } i \in I, \quad \text{then} \quad \prod_{i \in I} A_i \neq \emptyset \tag{1}$$

where $I = \{1, 2, \ldots, n\}$, be extended to the case of arbitrary (and therefore possibly infinite[†]) $I$?

The *axiom of choice*, AC, says yes.

**IV.1.1 Axiom (Axiom of Choice, or AC).** *If $I$ and $A_a$, for all $a \in I$, are nonempty sets, then $\prod_{a \in I} A_a \neq \emptyset$.*

But why "axiom"? After all, the case for finite $I$ is provable as a theorem, that is, (1) above. Before we address this question, let us first consider some more down-to-earth equivalent forms of AC.

**IV.1.2 Theorem.** *The following statements* (1), (2), (3)*, and* (4) *are provably equivalent.*

(1) AC.

(2) *If the* set *$F$ is a nonempty family of nonempty sets, then there is a function $g$ such that* $\mathrm{dom}(g) = F$ *and $g(x) \in x$ for all $x \in F$.*

[†] The terms "infinite" and "finite" throughout this discussion have their intuitive metamathematical meaning.

(3) *If the* set $S$ *is a relation, then there is a function* $f$ *such that* $\mathrm{dom}(f) = \mathrm{dom}(S)$ *and* $f \subseteq S$.

(4) *If the* set $F$ *is a nonempty family of* pairwise disjoint *nonempty sets, then there is a set* $C$ *that consists of exactly one element out of each set of* $F$ (*i.e., for each* $x \in F$, $C \cap x$ *is a singleton*).

**Note.** The function $g$ in (2) above is called a *choice function* for $F$.

*Proof.* (1) → (2): Given a set $F$ as in (2). Define $i \overset{\text{def}}{=} \lambda x.x$ with $\mathrm{dom}(i) = F$. Then $F$ can be viewed as the *indexed* family $(i(x))_{x\in F}$, or $(x)_{x\in F}$. By (1) there is a $g \in \prod_{x\in F} x$. Thus, $\mathrm{dom}(g) = F$ and $g(x) \in x$ for all $x \in F$.

(2) → (3): Given a relation $S$ (set). Let $F \overset{\text{def}}{=} \{S\langle a\rangle : a \in \mathrm{dom}(S)\}$. $F$ is a set by III.8.9, since dom $S$ is a set (III.11.8). If $F = \emptyset$, then $S = \emptyset$ and $f = \emptyset$ will do. So let $F \neq \emptyset$. By (2), there is a choice function $g$, i.e., $\mathrm{dom}(g) = F$ and $g(x) \in x$ for all $x \in F$.[†] In terms of $S$, the last result reads $g\big(S\langle a\rangle\big) \in S\langle a\rangle$ for each $a \in \mathrm{dom}(S)$. Clearly, $f \overset{\text{def}}{=} \big\{\big\langle a, g\big(S\langle a\rangle\big)\big\rangle : a \in \mathrm{dom}(S)\big\}$ will do.

(3) → (4): Let $F$ be as in (4). Define $S \overset{\text{def}}{=} \{\langle x, y\rangle : y \in x \in F\}$.[‡] $S$ is a set, since $S \subseteq F \times \bigcup F$. Now apply (3) to obtain $f \subseteq S$ with $\mathrm{dom}(f) = \mathrm{dom}(S) = F$. Take $C = \mathrm{ran}(f)$, a set by III.11.28.

To verify, let $x \in F = \mathrm{dom}(f)$. Then $\langle x, f(x)\rangle \in S$; therefore $f(x) \in x$. This along with $f(x) \in C$ yields $f(x) \in C \cap x$. Let also

$$y \in C \cap x \tag{$i$}$$

Hence $y \in C$ in particular. Then, for some $z$, $f(z) = y$; therefore $\langle z, y\rangle \in S$ and thus $y \in z$. By ($i$), $y \in x \cap z$, so that $x = z$ (by the assumption on $F$). This yields $y = f(z) = f(x)$. Thus, $C \cap x = \{f(x)\}$.

(4) → (1): Let $(A_a)_{a\in I}$ be an indexed family of nonempty sets ($I \neq \emptyset$ as well). Let $F \overset{\text{def}}{=} \mathrm{ran}(\lambda a.(\{A_a\} \times A_a))$ for $a \in I$. $F$ is a set by III.11.28, and its members are pairwise disjoint sets; for if $A_a \neq A_b$, then $\langle A_a, x\rangle \neq \langle A_b, y\rangle$ for all $x$, $y$, and thus $(\{A_a\} \times A_a) \cap (\{A_b\} \times A_b) = \emptyset$. By (4) there is a set $C$ such that $C \cap (\{A_a\} \times A_a)$ is a singleton for all $a \in I$.

Define $f \overset{\text{def}}{=} \big\{\langle a, \delta(y)\rangle : \langle a, y\rangle \in I \times \big(C \cap (\{A_a\} \times A_a)\big)\big\}$, which is a set by III.8.9, and obviously a function by the previous remark. Now, $\mathrm{dom}(f) = I$

[†] $x \in F \leftrightarrow (\exists a \in \mathrm{dom}(S))x = S\langle a\rangle$ (cf. III.8.7).

[‡] By "$y \in x \in F$" I mean "$y \in x \wedge x \in F$", i.e., using $\in$ conjunctionally.

and $f(a) = \delta(y) \in A_a$ for all $a \in I$; hence $f \in \prod_{a \in I} A_a$, that is, $\prod_{a \in I} A_a \neq \emptyset$. □

We will concentrate on the equivalence of AC with (4), due to the latter's intuitive appeal. Is now (4) "really true"? Is it possible to *choose* one element out of *each* set $x$ of a possibly infinite[†] set $F$ of nonempty pairwise disjoint sets, in order to form a set $C$? In the finite case we *can* literally "choose" each representative from each $x \in F$, for if there are $n$ such choices, we can fit them in a proof that is about $n$ lines long (see the proof of (1) at the closing of Chapter III). We cannot do the same in the infinite case, for proofs must have finite length. Of course, it often happens that we can *describe* an infinite process – such as an infinite sequence of choices – in a finite manner. For example, if $F$ consists exclusively of nonempty subsets of $\mathbb{N}$, then we can *define* $C$ compactly without having to list our infinite set of choices: $C \overset{\text{def}}{=} \{y : y \text{ is smallest in } x \wedge x \in F\}$.

One point of view maintains that to accept the existence of a set like $C$ we must be able to give a "rule" or "unambiguous definition" $\mathscr{P}[y]$ – just as in the example above. Holders of this viewpoint do not accept AC as a legitimate axiom. They argue that in the absence of "structure" in the set members $x$ of $F$, all the elements of such $x$ "look alike", and therefore the infinite process of "choosing" cannot be compacted into a finite well-defined description. This is true even for very small sets $x$ (it is the size of $F$, not that of $x \in F$, that creates the problem).[‡]

A well-known example due to Russell contrasts an infinite set of pairs of shoes with an infinite set of pairs of socks. In the former case the set $C$ can be defined compactly to consist of, say, the left shoe out of each pair. In the case of socks this "rule" does not define well which sock to pick, because, even though they are distinct objects, the two socks in a pair cannot be distinguished by "left" vs. "right".

The other philosophical point of view accepts that sets exist outside ourselves despite our frequent inability to define them "well", or to describe them. Thus, the choice set $C$ is some arbitrary "partition"[§] of the objects of "real" mathematics into members (of $C$) and non-members. As such, it exists whether we can define it well or not.[¶]

[†] Intuitively speaking, for now.

[‡] If each $x \in F$ is a singleton, then, of course, $C$ can be well defined.

[§] We do not attach any technical significance to the term "partition" here.

[¶] It is conceivable that someone some day may come up with a way to describe how to choose one sock from each one of an infinite collection of sock pairs. It would be therefore unwise to say "it cannot be done" simply because you or I cannot do it today.

Under this Platonist interpretation of "existence", a set of representative socks, one out of each pair in an infinite set of pairs, certainly exists. More generally, (4) and, equivalently, AC are "true".[†]

## IV.2. More Justification for AC; the "Constructible" Universe Viewpoint

Throughout this section we reason Platonistically in the domain of informal (or "real") set theory. Within the set-formation-by-stages doctrine we can argue the reasonableness of AC, paraphrasing Gödel's proof of the consistency of AC with the remaining axioms of ZF (Gödel (1939, 1940)).

Let us take seriously the challenge that AC does not provide us with a *well-defined* "rule" to effect the potentially infinitely many choices. Thus, for the balance of this section we will respond by demanding that *all* sets – not just those that AC asserts to exist – be "given" by a well-defined rule. This just levels the playing field.

In particular, when we apply the power set operation, $\mathbf{P}(A)$, to an infinite set $A$, we will accept that only those subsets of $A$ that are "well-definable" *exist* (i.e., as *sets*; we will soon make this requirement precise).[‡]

This attitude is similar to the one that separates collections into sets and proper classes: That some collections are not sets is a situation we are by now comfortable with. In this section we further narrow down what collections we will accept as sets in defense of AC.

This is a *local* restriction, however, valid only in this section. In the remainder of the volume we revert to our understanding of "real" sets as this was explained in Chapter II (II.1.3).

[†] The reader will observe that all we are doing here is arguing that a proposed new axiom is *reasonable*. This is a process we have been through for all the previous axioms, and it does not constitute a proof of the axioms in the metatheory. The notion "reasonable" is not temporally stable. When Cantor introduced set theory, the entire theory was "unreasonable" to many mathematicians of the day – including influential ones like Poincaré, who suggested that most of Cantor's set theory ought to be discarded. When Russell proposed to found mathematics on logic, this too was considered as an "unreasonable" point of view. For example, Poincaré protested that this was tantamount to suggesting that the whole body of mathematics was just a devious way to say $\mathscr{A} \leftrightarrow \mathscr{A}$. As mathematics progresses, mathematicians become more ready to accept the reasonableness of formerly "unreasonable" concepts or statements.

[‡] "Well-definable" is just an emphatic way of saying "(first order) definable", in the sense that we can write these sets down as class terms. We have already remarked (cf. II.4.2(b)) that we cannot expect all subsets of $\mathbb{N}$ to be first order definable, for they are far too many of them.

The definition of the "well-definable" sets will be given by formulas of set theory. We hope to be able to "sort" all possible such formulas in "ascending order", indicating such an order by the symbol "$\prec$". Next, we will see that $\prec$ on formulas naturally induces an order on the defined sets. To avoid notational confusion, we will use the symbol "$\lhd$" for this induced order on sets. With some luck, $\lhd$ will arguably be a *well-ordering*, i.e., each nonempty class will have a minimum element (with respect to $\lhd$). If all this succeeds, we will have two things:

(1) A restricted universe of sets, $\mathbb{L}$, where all sets are *definable* (all the other sets are ignored – banned from "sethood", that is).
(2) There will be a well-ordering, $\lhd$, on this restricted universe.

Thus, if $A$ is any set of nonempty sets, a choice function for $A$ can be (well) defined by setting $f(x)$ equal to the minimum $a \in x$ with respect to the ordering $\lhd$.

To begin with, we will need a judicious *re*interpretation of what is going on at each stage of set construction.

A stage of set construction is one of two possible types: a *collecting* type, or a *powering* type.

At a *collecting stage* one collects into a set all the objects that are available so far. In particular, since the urelements are given outright, the 0th stage is a collecting stage, at which the set of all urelements, call it $M$, is formed. At any subsequent collecting stage, we form the union of all the sets that were formed at all previous stages.

At a *powering stage* we form the set of all well-definable subsets of the set formed at the immediately previous stage – a sort of truncated power set.

The stages occur in the following order, defined inductively:[†]

(i) The 0th stage is a collecting stage at which the set of all urelements, $M$, is formed.
(ii) If at the arbitrary collecting stage the set $X$ has been formed, then this stage is followed *immediately* by infinitely many powering stages, to form the sets $X_1, X_2, \ldots, X_n, \ldots$, where

$$X_1 = \mathbf{D}(M \cup X) \quad \text{and,} \quad \text{for } n \geq 1 \quad X_{n+1} = \mathbf{D}(M \cup X_n) \qquad (1)$$

[†] The following informal definition is adequate for our informal discussion. A precise version will be given with the help of *ordinals* – formal counterparts of "stages" – when we revisit the constructible universe in Chapter VI.

In (1), $\mathbf{D}(A)$ denotes the set of all *definable* subsets of $A$. We will soon make the meaning of the term $\mathbf{D}(A)$ precise, but for the time being let us imagine that it is a pared-down version of $\mathbf{P}(A)$, that is, $\mathbf{D}(A) \subset \mathbf{P}(A)$ for infinite sets $A$.[†]

(iii) Immediately after each such infinite sequence of powering stages, a collecting stage occurs to form the union of all the sets formed at all the previous stages.

This process, alternating between (ii) and (iii), continues *ad infinitum* and constructs *all sets* (all *definable* sets really, but you will recall that in this section we pretend that these are the only legitimate sets anyway).

**IV.2.1 Remark.** The need for collection, after each sequence of powering, should be clear. For example, if we stop the process after the first sequence of powering, then, even though we have constructed sets with arbitrary integer depth of nesting of $\{\}$-brackets, we have not constructed a *single* set that contains as elements sets with all possible depths of nesting of $\{\}$-brackets.

Specifically, if $X_1, X_2, \ldots, X_n, \ldots$ constitutes the *first* sequence of powering, then

$$\emptyset \ \in X_1$$

and for $n \geq 1$,

$$\underbrace{\{\ldots\{}_{n}\emptyset\underbrace{\}\ldots\}}_{n} \in X_{n+1}$$

But *none* of the $X_i$ contains *all* of the

$$\underbrace{\{\ldots\{}_{n}\emptyset\underbrace{\}\ldots\}}_{n}$$

for all $n$. □

It is useful to observe the following important property of each set $Y$ constructed at some stage: *If* $x \in y \in M \cup Y$, *then* $x \in M \cup Y$.[‡]

The claim is trivially true if $y$ is an atom (see the previous footnote).

[†] Of course, in principle, we can list explicitly *all* subsets of any finite set, so that for finite sets $A$ we intuitively accept that all their subsets are definable, i.e., $\mathbf{D}(A) = \mathbf{P}(A)$ in this case.

[‡] A set $S$ that satisfies $a \in b \in S \rightarrow a \in S$ – that is, $a \in b \wedge b \in S \rightarrow a \in S$ – is called *transitive*. Such sets play a major role in set theory – all ordinals are transitive, to make the point. Here are two simple examples:

(a) $\{\#, ?\}$, where # and ? are urelements ($a \in b \in S \rightarrow a \in S$ is true for $b$ an urelement, since then $a \in b \in S$ is false)

(b) $\{\emptyset, \{\emptyset\}\}$.

We say "true" and "false" freely in this section, since we are working, like Platonists, in the metatheory.

If $y$ is a set, then we rephrase what we want to prove as follows:

$$y \in M \cup Y \rightarrow y \subseteq M \cup Y \tag{2}$$

We prove (2) by induction on stages (that we went through towards building $Y$). To this end, we need to verify the following:

(i) The set $Y$ constructed at the 0th stage has the property.
(ii) The property propagates with collecting.
(iii) The property propagates with powering.

As for (i), this is true because the $Y$ formed at stage 0 is $M$, and $M$ is transitive (see the footnote to the claim) – or, another way of saying this, $y \in M \cup Y$ is false ($M \cup Y = M$ contains only atoms, while $y$ is a set).

As for (ii), let $Y = \bigcup\{Z, W, \ldots\}$ be formed at a collecting stage, where $Z, W, \ldots$ are *all* the sets formed at all the previous stages. Let $y \in M \cup Y$. Thus, $y \in Y$ (for $M$ contains only atoms); hence

$$y \in \text{ (say) } W \subseteq M \cup W$$

By the induction hypothesis (I.H.), $y \subseteq M \cup W$, and, since $W \subseteq Y$, it follows that $y \subseteq M \cup Y$.

As for (iii), let $Y = \mathbf{D}(M \cup X)$, where $X$ is the set we have built at the immediately previous stage. Let $y \in M \cup Y$ be true and take any $x \in y$. Again, $y \in Y$, thus $y \subseteq M \cup X$, hence $x \in M \cup X$.

Now, if $x \in M$, then $x \in M \cup Y$. If not, then $x$ is a set, and I.H. yields $x \subseteq M \cup X$, from which follows $x \in Y$. Thus, in either case, $x \in M \cup Y$, and ($x$ being arbitrary) $y \subseteq M \cup Y$.

**IV.2.2 Remark.** We state an important by-product of the transitivity of the sets $M \cup X$, where $X$ has been obtained in our construction. If $Y = \mathbf{D}(M \cup X)$ for some such $X$, then we have that

$$X \subseteq M \cup Y$$

Indeed, let $x \in X$. If $x \in M$, then we are done. Else, $x$ is a set and $x \in M \cup X$; therefore $x \subseteq M \cup X$. It follows that $x \in Y$. □

We now turn to how the sets obtained at powering stages are actually "defined". Let us "sort" in an arbitrary *fixed* way the alphabet of the first-order language of logic that we have been using all along (we will use the symbol $\prec$

to indicate the assumed order on the alphabet, $\mathscr{A}$, of logical and nonlogical symbols). Now,

$$\mathscr{A} = \{\forall, \exists, \neg, \wedge, \vee, \rightarrow, \leftrightarrow, =, (, ), v, |, \in, U\}$$

where the symbols $v$ and $|$ are used to build the object variables $v_0, v_1, v_2, \ldots$ as $v|v$, $v||v$, $v|||v, \ldots$ (as usual, we can use abbreviations such as $x$, $y$, $z$ – with or without primes or subscripts – for variables). Let us fix the order

$$\forall \prec \exists \prec \neg \prec \wedge \prec \vee \prec\rightarrow\prec\leftrightarrow \prec=\prec(\prec) \prec v \prec | \prec\in\prec U \tag{3}$$

for $\mathscr{A}$.

We next augment our alphabet to include the *names* $\widehat{0}, \widehat{1}, \widehat{2}, \ldots, \widehat{n}, \ldots$ of all urelements,[†] and exactly *one* name for each *definable*[‡] set.

As a matter of notation, if $c$ is (I mean, informally names) a definable set, then $\widehat{c}$ will denote the unique name for $c$ that we *import* into our alphabet $\mathscr{A}$. In particular, the horrible notation $\vec{\widehat{c}}_n$ will stand for the sequence of names $\widehat{c}_1, \ldots, \widehat{c}_n$.

[†] It might be thought – with some justification – that we are cheating somewhat here by taking $M$, the set of all urelements, to be $\mathbb{N}$. Recall however that all that we are after is to

(1) give a philosophically plausible description of what sets are, and
(2) within this description argue that AC holds.

In other words, following Gödel, we are proposing an *informal* and plausible universe of "real" sets.

We have chosen $\mathbb{N}$ as the set of urelements because AC holds on it by the least integer principle. How well does this choice hold philosophically, i.e., how well are we serving requirement (1) above? Well, it should not be too difficult to accept the view that the primeval "real stuff" of mathematics – the atomic objects – is the natural numbers, and that all else in mathematics we build starting from these numbers. After all, one of the most careful among the fathers of foundations, Kronecker, had no trouble with this position at all. He is said to have held that "God created the integers; all else is the work of man". Mind you, Kronecker, the mentoring father of intuitionism and a confirmed finitist, did not allow for the entire set of natural numbers, but only granted you the right of having as many numbers as you wanted by simply adding one to the last one you have had.

Even technically, one can argue that the choice of such a small set of urelements does not restrict our ability to use sets to do mathematics, for it turns out that even a smaller set works (i.e., leads to a set theory that is sufficiently rich for the purposes of doing mathematics). Namely, as we shall see in Chapter V, von Neumann has shown how to build the natural numbers and, therefore, also Kronecker's "all else", starting from $\emptyset$.

[‡] Definable in the process that we are describing. By the way, introducing a unique name for each "real object" of a collection is a trick that we have already used in describing the semantics of first order languages in I.5.4.

Our goal is to extend the order $\prec$ from $\mathscr{A}$ to all names, and then to induce it on the *named objects*, that is, all objects of our definable universe.

Thus, what we have set out to do is to achieve

$$a \lhd b \quad \text{iff} \quad \widehat{a} \prec \widehat{b} \tag{4}$$

We do this in stages, starting by extending (3) into

$$\forall \prec \exists \prec \neg \prec \wedge \prec \vee \prec \rightarrow \prec \leftrightarrow \prec = \prec ( \prec ) \prec v \prec \mid \prec \in \prec U \prec \widehat{0} \prec \widehat{1} \prec \cdots \tag{5}$$

It is trivial that $\prec$ *in its present stage of definition* given by (5) is a *well-ordering*, that is, every nonempty set of symbols in $\mathscr{A} \cup \{\widehat{n} : n \in \mathbb{N}\}$ has a $\prec$-smallest element.[†]

**IV.2.3 Definition.** A set $a$ is *definable* from $X$, a formula $\mathscr{P}(v_0, v_1, \ldots, v_n)$ over the initial alphabet (3), and the parameters $\vec{\widehat{b}}_n$ iff

$$a = \{x \in X : \mathscr{P}(\widehat{x}, \vec{\widehat{b}}_n) \text{ is true in } X\}$$

where the (constant) objects $b_i$, named by $\widehat{b_i}$, are all in $X$.

"Is true in $X$" means that the truth value is "computed" by restricting all bound variables of the sentence $\mathscr{P}(\widehat{x}, \vec{\widehat{b}}_n)$ to vary over $X$.[‡] That is, an occurrence of $(\exists y)$ or $(\forall y)$ in the formula means $(\exists y \in X)$ or $(\forall y \in X)$ respectively.

$\mathbf{D}(X)$ denotes *all* sets $a$ definable from $X$ and parameters in $X$ (for *all* $\mathscr{P}$ over the initial alphabet (3)). □

We will well-order the class of all definable sets by well-ordering their definitions.

We do not append all the names $\widehat{c}$ to $\mathscr{A}$ at once. We have only appended the names of the atoms so far to form the alphabet (5). There are two good reasons for this: One, we will augment our formal symbol set by stages, so that as it grows it stays (provably) well-ordered. Two, we will add a name only after its corresponding set has been seen to be definable; for, conceivably, not all sets are definable.

[†] Well-orderings will be studied in detail in Chapter VI.

[‡] Why $\widehat{x}$ in $\mathscr{P}(\widehat{x}, \vec{\widehat{b}}_n)$? This is because each object $x \in X$ that we check for membership in $a$ enters the defining formula $\mathscr{P}$ via its *name*.

In order to keep the notation simple as we append more symbols, we will continue naming the so augmented alphabet "$\mathscr{A}$". Thus, (5) depicts the version of $\mathscr{A}$ that we have immediately after appending the names of all the atoms to the initial alphabet (3).

As usual, $S^+$ denotes the set of all nonempty strings of symbols from $S$, while $S^i$, for $0 < i \in \mathbb{N}$, denotes the set of strings of length $i$.[†] Thus, $S^+ = \bigcup_{i \geq 1} S^i$ (cf. I.1.4).

**IV.2.4 Lemma.** *Let $\prec$ be a well-ordering on the set $S$. We extend $\prec$ to $S^+$ by the following rules, but still call it $\prec$.*

- *We order by increasing string length, i.e., all the elements of $S^i$ precede those of $S^{i+1}$.*
- *In each equal-length group (i.e., each $S^i$) we order the strings* lexicographically *(as in dictionaries), that is, of two unequal strings, the smaller is the one that in the leftmost position of disagreement contains the smaller of the two disagreeing symbols of $S$.*

*Then $\prec$ on $S^+$ is a well-ordering.*

*Proof.* Let $\emptyset \neq C \subseteq S^+$. Pick any string $a_1 a_2 \ldots a_n$ of *shortest length $n$*. We define a sequence of transformations:

$$\text{Transform } a_1 a_2 \ldots a_n \text{ to } \widetilde{a}_1 a_2 \ldots a_n$$

where $\widetilde{a}_1$ is the $\prec$-*smallest* in $S$ ($S$ is well-ordered!) such that $\widetilde{a}_1 a_2 \ldots a_n \in C$.[‡] In general, assuming that $\widetilde{a}_1 \widetilde{a}_2 \ldots \widetilde{a}_i a_{i+1} \ldots a_n \in C$ has been defined,

$$\text{Transform } \widetilde{a}_1 \widetilde{a}_2 \ldots \widetilde{a}_i a_{i+1} \ldots a_n \text{ to } \widetilde{a}_1 \widetilde{a}_2 \ldots \widetilde{a}_i \widetilde{a}_{i+1} \ldots a_n$$

where $\widetilde{a}_{i+1}$ is the $\prec$-smallest in $S$ such that $\widetilde{a}_1 \widetilde{a}_2 \ldots \widetilde{a}_i \widetilde{a}_{i+1} \ldots a_n \in C$.

Thus, we have defined, by induction on $i$ ($\leq n$), a $\prec$-smallest element $\widetilde{a}_1 \widetilde{a}_2 \ldots \widetilde{a}_n$ of $C$. □

**IV.2.5 Corollary.** *For the version of $\mathscr{A}$ given by* (5), *$\mathscr{A}^+$ is well-ordered by $\prec$.*

[†] Of course, a string over $S$ of length $i$ is just a member of the $i$-copy Cartesian product $S^i$: $\langle x_1, \ldots, x_i \rangle$. One usually writes strings without the angular brackets, and without the comma separators, like this: $x_1 x_2 \ldots x_i$. Naturally, if the latter notation becomes ambiguous – e.g., if $S = \{0, 00\}$ then 00 might be either $\langle 00 \rangle$ or $\langle 0, 0 \rangle$ in vector notation – then we revert to the vector notation.

[‡] $\widetilde{a}_1$ may be the same as $a_1$.

So far, we have *at stage* 0:

- a well-ordering of $M$, $\lhd$, *defined* to be equal to the "standard $<$" on the set of atoms (since $M = \mathbb{N}$), and
- a relation $\prec$ satisfying (4) on $M$ because of (5).

This observation validates the basis of the induction on stages that we now embark upon.

Assume then that $\lhd$ has been extended to a well-ordering on the set of all objects $M \cup X$ defined so far, in such a way that (4) holds, where $\prec$ is a well-ordering on the set of all symbols and names *that we have up to now* – this augmented set is still called $\mathscr{A}$ – and moreover assume that the present stage to be "executed" is a powering stage that will yield $Y = \mathbf{D}(M \cup X)$.

We now extend $\lhd$ to $Y$ by cases:

Let $\{a, b\} \subseteq Y$.

*Case 1.* $\{a, b\} \subseteq X$. (This is a legitimate case by Remark IV.2.2.) Then, $a \lhd b$ is already defined, and *we do not alter it*. By I.H., (4) holds.
*Case 2.* $a \in X$ and $b \notin X$. Then define $a \lhd b$ and $\widehat{a} \prec \widehat{b}$. Thus (4) still holds.
*Case 3.* $a \neq b$, where $a \notin X$ and $b \notin X$ (i.e, both are "new" objects – hence sets). Let

$$a = \{x \in M \cup X : \mathscr{P}(\widehat{x}, \vec{\widehat{a}}_n) \text{ holds in } M \cup X\} \tag{6}$$

and

$$b = \{x \in M \cup X : \mathscr{Q}(\widehat{x}, \vec{\widehat{b}}_m) \text{ holds in } M \cup X\} \tag{7}$$

where the parameters $a_i$ and $b_j$ are in $M \cup X$.

By Corollary IV.2.5, $\prec$ extends from $\mathscr{A}$ to $\mathscr{A}^+$ as a well-ordering.

Now, every definable set will be defined infinitely many times in this process.[†] Thus, to extend $\prec$ and $\lhd$ by adding to them the pairs $\langle \widehat{a}, \widehat{b} \rangle$ and $\langle a, b \rangle$ – or $\langle \widehat{b}, \widehat{a} \rangle$ and $\langle b, a \rangle$, as the case may be – respectively, we look, in a sense, for the "earliest construction times" for $a$ and $b$, or, more conveniently, for the *$\prec$-smallest definition*.

(i) Of all the possible formulas $\mathscr{P}(v_0, \vec{v}_n)$ – over the initial alphabet (3), with free variables $v_0, \ldots, v_n$ – that can define the set *a at this stage* via appropriate parameters, denoting members of $M \cup X$, substituted into the variables,

[†] For example, a defining formula $\mathscr{P}$ defines the same set as $\mathscr{P} \vee \mathscr{P}$, or $\neg\neg\mathscr{P}$, etc., or any other formula $\mathscr{Q}$ for which the equivalence $\mathscr{P} \leftrightarrow \mathscr{Q}$ holds, trivially or not.

we choose the $\prec$-smallest in (6). Similarly, of the possible $\mathscr{Q}(v_0, \vec{v}_m)$ that can define the set $b$ at this stage, we choose the $\prec$-smallest in (7). This invokes IV.2.5.

(ii) Of the possible parameter *strings* $\widehat{a}_1\widehat{a}_2 \ldots \widehat{a}_n$ that work in conjunction with the formula $\mathscr{P}(v_0, \vec{v}_n)$ chosen in (i) above to define $a$ as in (6), we choose the $\prec$-smallest. Similarly for $b$. This also invokes IV.2.5.

After having exercised all this caution, and having chosen $\mathscr{P}$, $\mathscr{Q}$, $\vec{\widehat{a}}_n$, and $\vec{\widehat{b}}_m$ as directed in (i) and (ii) above, we extend $\lhd$ and $\prec$ by defining

$$a \lhd b \text{ and } \widehat{a} \prec \widehat{b} \quad \text{iff} \quad \begin{cases} \mathscr{P}(v_0, \vec{v}_n) \prec \mathscr{Q}(v_0, \vec{v}_m), \\ \qquad\qquad \text{or} \\ \mathscr{P}(v_0, \vec{v}_n) \equiv \mathscr{Q}(v_0, \vec{v}_m) \text{ (equal as strings),} \\ \qquad\qquad \text{and } \widehat{a}_1\widehat{a}_2 \ldots \widehat{a}_n \prec \widehat{b}_1\widehat{b}_2 \ldots \widehat{b}_m \end{cases}$$

where the $\prec$ to the right of "iff" is meaningful, since the involved strings are in $\mathscr{A}^+$. The "normalization" of $\mathscr{P}$ and $\mathscr{Q}$ used in (6) and (7) ensures that the extension of $\lhd$ (and hence of $\prec$) is well defined, and is still a well-ordering, since the $\prec$ to the right of "iff" is.

This settles the induction step with respect to powering stages – having extended $\lhd$ to $Y$ so that (4) holds.

Suppose finally that the stage we are about to execute is a collecting stage that builds $Y$ as $\bigcup\{X, W, Z, \ldots\}$. By I.H., $\lhd$ is a well-ordering on each of $X, W, Z, \ldots$.

Let $a, b$ be in $Y$. Then $a, b$ are in $X$, say. Then $a \lhd b$ is already defined and satisfies (4); thus we need do nothing further.[†]

This concludes the definition of $\lhd$ as a well-ordering of the *entire class of definable sets and atoms*, $\mathbb{L}$.

We have obtained more than what we set out to achieve:

**IV.2.6 Metatheorem (Strong,** or **Global, Choice).** *If $\mathbb{F}$ is any class*[‡] *of mutually disjoint nonempty sets $R, S, \ldots$, then there is a class $\mathbb{T}$ that consists of exactly one element from each of $R, S, \ldots$.*

[†] Since $\lhd$ is updated only at powering stages as new sets get constructed, it is never redefined during the normalization (i) and (ii) above. Thus it cannot be that $a \lhd b$ in $X$ while $\neg a \lhd b$ in, say, $W$ above. The reader will also observe that IV.2.2 validates our contention that $a$ and $b$ are both in some earlier "$X$".

[‡] Not just set.

*Proof.* Put in $\mathbb{T}$ the $\lhd$-smallest element out of each $x \in \mathbb{F}$. □

**IV.2.7 Corollary.** AC *holds in* $\mathbb{L}$.

*Proof.* If $\mathbb{F}$ is a set, then so is $\mathbb{T}$ by collection (e.g., III.11.28, p. 206). □

**IV.2.8 Remark.** (1) Our notational apparatus does not allow higher order objects that are collections of (possibly) proper classes. If for a minute such objects were allowed, and if $\Sigma$ is one of them and it happens to contain mutually disjoint nonempty *classes* (not just sets), then a higher order collection $\mathbf{T}$ exists which contains exactly one element out of each $x \in \Sigma$. Just use the $\lhd$-smallest out of each $x$.

(2) Informally, we have established the acceptability (= informal "truth", modulo some appropriate understandings of what the real sets really are and how they come about) of a strong choice principle, and hence of AC. We did this under two opposing "philosophies" regarding set existence, a Platonist's approach (p. 217) and, subsequently, a definability or constructibility approach.

It must be conceded that under the philosophy "existence = definability", even though the argument itself that $\lhd$ exists and is a well-ordering of the universe is sound and can be promoted into a rigorous proof within formal set theory once we learn about ordinals, the background hypotheses could be attacked on the grounds that "real" sets might not be constructed in the manner we have assumed. The whole argument was a "what if".[†] In particular, there might be dissent on the choice of urelements, on what is going on at stages, on the use of exclusively first order formulas in *defining* sets, etc.

Let us be content with the fact that at least the *plausibility* if not as much as "proof" of a strong AC has been established under this philosophy, because the picture suggested of what sets are is intuitively pleasing and natural.

(3) In an axiomatic approach to set theory one adopts certain basic axioms which are *plausible* (or, more boldly, "true") and *adequately describe* our *a priori* perception of the nature of sets. The latter means that the axioms must also be sufficiently strong to imply as many "true" statements about sets as possible.

There are two difficulties regarding these requirements. The first is a technical difficulty, pointed out by Gödel (incompleteness theorem), namely, that there

[†] That is, a construction of a *model* for ZFC. The reader will note that in this "model" we only verified AC. Of course, one must verify *all* the nonlogical axioms in order to claim that a structure *is* a model. However, since we will revisit the constructible universe formally we chose here to only deal with our immediate worry: the "truth" of our newest axiom, AC.

are axiomatic theories (set theory – unfortunately – being one such) which are *incompletable*, i.e., as long as they are consistent, they can never capture all the true sentences that they are intended to capture (as theorems), no matter how many axiom schemata we add (even an infinite number, as long as the formulas that are axioms are recognizable as such).

The other difficulty has to do with limitations of our intuition (of course, intuition advances and becomes more permissive as mathematical culture develops). We do not know *a priori* what statements are supposed to be true (a good thing this: otherwise mathematicians would be out of business), and counterintuitive consequences of otherwise perfectly plausible axioms (shall I say "true"?) may unfairly reflect badly on the axioms themselves, in any mathematical culture that is not of sufficiently high order for mathematicians to know better.

That "perfectly acceptable" axioms can lead to theorems that will seriously challenge one's intuition cannot be better illustrated than by Blum's *speed-up theorem*[†] in computational complexity theory. This theorem follows from the only two axioms of the theory, both of which are outright "true".

The theorem says that there is a computable function $f$ on $\mathbb{N}$ with values in $\{0, 1\}$ which is so difficult to compute that for any program that computes $f$ there is another program that computes it *significantly faster* for all but finitely many inputs – in other words, there is no "best" program for $f$. Now, this result is certainly in conflict with intuition, but acceptable it must be, for the axioms in this case are unassailable.

Acceptability of AC was initially hampered by a similar phenomenon: It implied results that were unexpected and hard to swallow. The most notable such result was Zermelo's theorem that every set can be well-ordered, in particular that the set of reals can. See also the discussion in Wilder (1963, pp. 73–74); in particular note the concluding paragraph on p. 74.

To AC's defense, we observe that mathematics is not entirely innocent of counterintuitive constructions or theorems even in AC's absence. We have already noted Blum's theorem. Other examples are Weierstrass's construction of a continuous nowhere differentiable function, and Peano's space-filling curve (see Apostol (1957, p. 224)). Besides, we need AC because of vested interest. Without it, much of mathematics is lost. For example, the standard fact that *a countable union of countable sets is countable* crumbles if we disown AC (and this may come as a surprise to many readers).[‡]

[†] See Blum (1967), or Tourlakis (1984), where this theorem is rehearsed in detail.

[‡] Feferman and Levy (1963) have constructed a model of Zermelo-Fraenkel set theory *without* AC, where the reals $\mathbb{R}$, provably uncountable in ZF, are a countable union of countable sets.

(4) Two *formal* (i.e., syntactical) questions about AC must be settled right away:

(a) If ZF is consistent and we add AC to its axioms, is the new theory, ZFC, still consistent?
(b) Is AC provable in (i.e., a theorem of) ZF, *assuming* that ZF is consistent? (Of course, an inconsistent ZF would prove every formula, including the one that states AC (I.4.21).)

Gödel has answered (a) positively (1939, 1940; see also Devlin (1978)) by two different methods, constructing in ZF the *constructible universe* of sets (it is his first construction that we "popularized" within naïve set theory to define $\lhd$ in this section). On the other hand, Fraenkel and Mostowski (see Jech (1978a)) and Cohen (1963) answered question (b) *negatively*.

Thus, both AC and its negation are consistent with ZF, and one can take or leave AC without logical penalty either way. In this sense, AC has in the context of ZF the same status that Euclid's axiom on parallels has in the context of axiomatic geometry. Adopting or rejecting Euclid's axiom is just a reflection of what kind of geometry one wants to do. Similarly, adopting AC or not reflects the sort of set theory, and ultimately mathematics, one wants to do.

As we have indicated earlier, it makes sense to take a more direct approach to our choice of axioms (rather than the indirect, or "results-driven", approach), for it is easy to be misled by strange but correct results. If at all possible, we should adopt axioms by judging them *on their own plausibility* rather than on that of their consequences. On that count, AC is nowadays generally accepted without apology, since it is not any less plausible than, say, the axiom of replacement. It is noteworthy that the first order *logic* which Bourbaki uses as the foundation of his multi-volume work *Éleménts de Mathématique* contains a powerful "selection" axiom – using the $\tau$-operator (cf. Section I.6) – that directly turns the axiom of choice of set theory into a theorem. □ ☡☡

## IV.3. Exercises

**IV.1.** Show by an example that the assumption of pairwise disjointness is essential in the proof (3) → (4) of IV.1.2.

**IV.2.** Show that if for two objects $A$ and $B$ in $\mathbb{L}$ the formula $A \in B$ is true, then $A \lhd B$ is also true.

The following exercises are best approached after the reader has mastered the concepts of order and inductive definitions on ordered sets (Chapter VI). They are presented here because of their thematic unity with the concepts of the present chapter. The Kuratowski-Zorn version of AC is particularly useful in many branches of mathematics.

The reader is encouraged to try them out *informally*.

**IV.3.** AC implies that (Zermelo's well-ordering theorem) *every nonempty set $A$ can be well-ordered*, i.e., an order $<$ can be defined on $A$ so that every nonempty $B \subseteq A$ has a $<$-minimal element $b$ (that is, $\neg(\exists x \in B)x < b$). (*Hint.* Follow Zermelo's (1904) proof. Do not use the overkill of ordinals (VI.5.50). Instead, let $f$ be a choice function on $F = \mathbf{P}(A) - \{\emptyset\}$. Let $B \in F$ be called *distinguished* if it can be well-ordered by some order $<_B$ so that, for every $b \in B$, $b = f(A - \{x \in B : x <_B b\})$ (we call $\{x \in B : x <_B b\}$ a *segment* (in $B$), the one that is *determined* by $b$). For example, $\{f(A)\}$ and $\{f(A), f(A - \{f(A)\})\}$ are distinguished (in the latter, of course, we set $f(A) < f(A - \{f(A)\})$. Show that for any two distinguished sets $B$ and $C$, one is a segment of the other, if they are not identical (think of a maximal common segment; $\{f(A)\}$ is certainly a common segment). Take then the union of all distinguished sets, and compare with $A$.)

**IV.4.** A *linearly* or *totally* ordered set $A$ is one equipped with an order $<$ such that for any $a, b$ in $A$ it is true that $a = b \vee a < b \vee b < a$.

Formally, we proclaim that $< : A \to A$ is a linear order if we we have a proof of (or have assumed) $(\forall a)(\forall b)(a = b \vee a < b \vee b < a)$.

Show that if every set can be well-ordered, then (Hausdorff) in every set $A$ ordered by, say, $<$, every *totally* ordered subset $B$ is included ($\subseteq$) in a *maximal* totally ordered subset $M$ of $A$.

*Note.* Maximality means that if $a \in A - M$, then for some $m \in M$ neither $a < m$ nor $m < a$.

(*Hint.* If $B = A$, there is nothing to prove. Else, let $<_W$ be a well-ordering of $A - B$ (which in general has no relationship to $<$ that is already given on $A$). By induction on $<_W$, partition $A - B$ into a *good* and a *bad* set: Put the $<_W$-minimum element of $A - B$ in the good one if it is $<$-comparable with all $x \in A - B$; else put it in the bad one. If all the elements of $\{x \in A - B : x <_W a\}$ have been so placed, then place $a$ in the good set if it is $<$-comparable with all the elements in $A$ *and* good; else put it in the bad one.)

**IV.5.** Show that the italicized statement that follows (due to Kuratowski and Zorn; also known as "Zorn's lemma") is a consequence of Hausdorff's theorem in Exercise **IV.4** above. *If every totally ordered subset $B$ of an ordered (by $<$) set $A$ has an* upper bound *(that is, an element $b \in A$ such*

*that $x \in B$ implies $x = b$ or $x < b$; in short, $x \leq b$), then for every element $x \in B$ there is a $<$-maximal element $a$ of $A$ such that $x \leq a$.*
*Note.* $a$ above is $<$-maximal in $A$ in the sense that $\neg(\exists x \in A)a < x$.

**IV.6.** Show that the Kuratowski-Zorn theorem in Exercise **IV.5** above implies AC. This shows the equivalence of all four: AC, the Zermelo well-ordering theorem, Hausdorff's theorem, and Zorn's lemma.
(*Hint.* Let $A \neq \emptyset$ be given. We want a choice function on $F = \mathbf{P}(A) - \{\emptyset\}$. There certainly are choice functions on some subsets of $F$ – on any finite subsets, as a matter of fact. Let $\mathscr{F}$ be the set (why *set*?) of all choice functions on subsets of $F$. For $f$, $g$ in $\mathscr{F}$ define the order $f < g$ to mean $f \subset g$. Next, argue that any totally ordered subset of $\mathscr{F}$ has an upper bound, and thus apply Zorn's lemma to get a $<$-maximal member $\psi$ of $\mathscr{F}$. Argue that $\psi$ is a choice function on $F$.)

# V

# The Natural Numbers; Transitive Closure

## V.1. The Natural Numbers

We are now at a point in our development where much would be gained in expositional smoothness were we to have a *formal counterpart* of $\mathbb{N}$ in set theory.

For example, the main result of the next section is that of the existence of the *transitive closure*, $\mathbb{P}^+$, of an arbitrary relation $\mathbb{P}$ (an important result that we will need in Chapter VI). We will prove that $\mathbb{P}^+ = \bigcup_{i=1}^{\infty} \mathbb{P}^i$.

This requires that we settle the questions

(1) what is $\mathbb{P}^i$, and
(2) what is $\bigcup_{i=1}^{\infty} \mathbb{P}^i$?

Now this issue is much more complex than dealing with *one* (or, in any case, "finitely" many) $\mathbb{P}^i$ at a time – like $\mathbb{P}^2$, $\mathbb{P}^{101}$, $\mathbb{P}^{123005}$ – which we *can* define, and use, formally without the need for a formal copy of $\mathbb{N}$. The trick of absorbing the informal number $i$ inside the *name* so that it is invisible in the theory was done before (and discussed, for example, on p. 12). For example, $\mathbb{P}^2 = \{\langle x, y\rangle : (\exists z)(y\mathbb{P}z \wedge z\mathbb{P}x)\}$.

Here we need to collect all the infinitely many $\mathbb{P}^i$ into a class, *and* to allow the formal system to "see" the *variable* $i$, in order to speak of "$\bigcup_{i=1}^{\infty} \ldots$", a short form of "$\{z : (\exists i$ in an appropriate ZFC set of $i$'s$)z \in \ldots\}$".

Clearly, this is true even if $\mathbb{P}$ is a set (a restriction we want to avoid); therefore we need to formalize the presence of the "natural number" $i$.[†]

A similar situation arises in computer programming: We can use "informal subscripts" $1, 2, 3, \ldots$ to denote several unrelated variables as $X1$, $X2$,

[†] When $\mathbb{P}$ is a set, things are a bit easier. We can then prove existence of $\mathbb{P}^+$ not by confronting $\bigcup_{i=1}^{\infty} \mathbb{P}^i$ but by avoiding it. See Exercise V.16.

$X3, \ldots$ but we *cannot* refer to these informal subscripts *within the programming formalism* to access, say, the $i$th variable $Xi$, since *the programming language does not see the* $i$ *inside the name*. For example,

```
**for** $i = 1$ **to** $n$ **do**
    $Xi \leftarrow i$
**end do**
```

just refers to *one* variable – named $Xi$ – at all times and it successively changes its value from 1 through $n$. It does *not* refer to variables (named) $X1, X2, \ldots, Xn$.

Now, if we use $i$ as a *formal subscript* as in a *subscripted variable* (or "array") $X[i]$ then the following refers to $n$ *different* variables, $X[1]$ through $X[n]$:

```
**for** $i = 1$ **to** $n$ **do**
    $X[i] \leftarrow i$
**end do**
```

We proceed now to introduce a formal counterpart of $\mathbb{N}$, denoted by the standard symbol $\omega$.

**V.1.1 Definition.** A set $A$ is *inductive* iff

$$\emptyset \in A \wedge (\forall x \in A) x \cup \{x\} \in A$$

For any set $x$, $x \cup \{x\}$ is called the *successor* of $x$. A set $y$ is *a successor* iff $y = x \cup \{x\}$ for some $x$. □

Thus "$A$ is inductive" is (represented by) a formula of set theory.

**V.1.2 Example.** An inductive set $A$ contains $\emptyset$, $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}$, and as we go on, applying the successor operation again and again, we increase the *depth of nesting* of $\{\}$-brackets by 1 at every step. So these depths are successively $0, 1, 2, \ldots$.

We can identify these depths of nesting with the natural numbers of our intuition. Better still, we can identify $\emptyset$, $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}$, etc., with the natural numbers (this is "better" because, unlike the nebulous "depth of nesting", these sets are objects of set theory). □

Of course we have to settle a few things. Does any inductive set really exist? Is it not possible that an inductive set might contain much more than what we would care to identify with natural numbers? In a way, the answers are "yes" and "yes" – the first by the "axiom of infinity", the second by the fact that we have "limit ordinals" larger than $\omega$. These are inductive sets that contain much more than just copies of the intuitive natural numbers (this will be better understood in Chapter VI).

**V.1.3 Axiom (Axiom of Infinity).** *There is an inductive set.* □

By the remark following V.1.1, the axiom is a formula of set theory. Because of Example V.1.2, an inductive set – if such a set "truly" exists – has as a subset a set of "aliases" of all the members of $\mathbb{N}$, so it is *intuitively infinite*; hence the axiom name is appropriate. Now why is the axiom "really true"? Because we can certainly construct each (real) set in the infinite sequence $\emptyset$, $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}, \ldots,$ for each integer depth of nesting $n \in \mathbb{N}$,[†] and put them all in a class. Now this class has the same size as the (real) set $\mathbb{N}$ (why?); hence it must be a set by the "size limitation doctrine" of Chapter III. Alternatively, we can say that since *collection* is "true" and $\mathbb{N}$ is a set, then $\operatorname{ran}(f)$ is also a set (III.11.28), where $f$ is the function with domain $\mathbb{N}$ that for each $n \in \mathbb{N}$ "outputs" the set in the sequence $\emptyset, \{\emptyset\}, \ldots$ that has depth of nesting of braces equal to $n$.

Furthermore, by construction, $\operatorname{ran}(f)$ is inductive.

It should be noted that the negation of the axiom of infinity is "no inductive sets exist", *not* "infinite sets do not exist" (see Exercise VI.54).

Finally, we should mention that it is known that Axiom V.1.3 is not provable by the axioms we have so far (again, see Exercise VI.54); therefore it is a welcome addition, being intuitively readily acceptable (and necessary).

**V.1.4 Lemma.** *If $\mathscr{F}$ is a nonempty family of inductive sets, then $\bigcap \mathscr{F}$ is an inductive set.*

*Proof.* Easy exercise. □

**V.1.5 Definition (The Formal Natural Numbers).** We introduce a new constant, $\omega$, in the language of set theory by the explicit definition

$$\omega = \bigcap \{x : x \text{ is an inductive set}\}$$

[†] To reach any set in the sequence that involves depth of nesting of { }-brackets equal to $n$, all we have to do is to write down a proof, of length $n + 1$, that starts with the statement "$\emptyset$ is a set" and repeatedly uses the lemma "since $x$ is a set, then so is $x \cup \{x\}$" (by union and pairing) as $x$ runs through $\emptyset, \{\emptyset\}, \ldots.$

We will call $\omega$ the set of *formal natural numbers* (we will drop the qualification "formal" whenever there is no danger of confusing $\mathbb{N}$ and $\omega$).

Members of $\omega$ are called (formal) natural numbers. In our metanotation $n, m, l, i, j, k$ – with or without primes or subscripts – default to (formal) natural number variables unless the context dictates otherwise.

That is, we are introducing *natural number typed variables* in our *argot*. Thus, "$(\forall m)\mathscr{P}[m]$" is short for "$(\forall x \in \omega)\mathscr{P}[x]$". "$(\exists m)\mathscr{P}[m]$" means "$(\exists x \in \omega)\mathscr{P}[x]$". □

By the axiom of infinity, $\omega$ is indeed a set (since $\{x : x \text{ is an inductive set}\}$ is nonempty). By Lemma V.1.4 it is itself inductive. Clearly, $\omega$ is the $\subseteq$-smallest inductive set, for if $A$ is inductive, then $A \in \{x : x \text{ is an inductive set}\}$ and hence $\omega \subseteq A$. This simple observation leads to

**V.1.6 Theorem (Induction over $\omega$).** *Let $\mathscr{P}(x)$ be a formula. Then*

$$\mathscr{P}(\emptyset), (\forall x)\big(\mathscr{P}(x) \to \mathscr{P}(x \cup \{x\})\big) \vdash (\forall x \in \omega)\mathscr{P}(x)$$

*Proof.* Assume the hypothesis. Let $B = \{x \in \omega : \mathscr{P}(x)\}$. By separation, $B$ is a set. The hypothesis (and the fact that $\omega$ is inductive) implies that $B$ is inductive. Hence ($\omega$ is smallest inductive set), $\omega \subseteq B$. That is, $x \in \omega \to x \in \omega \wedge \mathscr{P}(x)$; hence $(\forall x \in \omega)\mathscr{P}(x)$ by tautological implication followed by generalization. □

**V.1.7 Remark.** The induction over $\omega$ is stated in a more user-friendly way as "To prove $(\forall x \in \omega)\mathscr{P}(x)$ one proves

(1) $\mathscr{P}(\emptyset)$ (this is the *basis*), and
(2) *freezing* $x$, the hypothesis (*induction hypothesis*, or I.H.) $\mathscr{P}(x)$ implies $\mathscr{P}(x \cup \{x\})$."

Note that (2) above establishes $(\forall x)(\mathscr{P}(x) \to \mathscr{P}(x \cup \{x\}))$ by the deduction theorem (which uses the freezing assumption) followed by generalization.

The process in quotes proves $\mathscr{P}(x)$ *by induction on $x$* (*over $\omega$*). $x$ is called the *induction variable*.

Applying the deduction theorem to V.1.6, one derives the ZFC theorem,

$$\mathscr{P}(\emptyset) \to (\forall x)\big(\mathscr{P}(x) \to \mathscr{P}(x \cup \{x\})\big) \to (\forall x \in \omega)\mathscr{P}(x) \qquad \square$$

We develop a few properties of the formal natural numbers that we will need on one hand for our theoretical development, and on the other hand in order to make the claim that $\omega$ is a formal counterpart of $\mathbb{N}$ more acceptable.

**V.1.8 Lemma.** *$n \cup \{n\} \neq \emptyset$ for all $n \in \omega$.*

This corresponds to "$n + 1 \neq 0$" on $\mathbb{N}$, or **ROB**[†] axiom ***S*1**.

*Proof.* $n \in n \cup \{n\}$. □

**V.1.9 Lemma.** *$n \cup \{n\} = m \cup \{m\}$ implies $m = n$ for all $n, m$ in $\omega$.*

This corresponds to "$n + 1 = m + 1$ implies $n = m$" on $\mathbb{N}$, or **ROB** axiom ***S*2**.

The reader will note from the proof below that this result is valid for *all* sets $n, m$ not just those in $\omega$.

*Proof.* Let instead $\neg m = n$ (proof by contradiction, frozen $m$ and $n$). As $n$ is on the left hand side of

$$n \cup \{n\} = m \cup \{m\}$$

it must be on the right hand side too; hence, $n \in m$. Similarly, $m \in n$, and this contradicts the axiom of foundation (applied to $\{m, n\}$). □

**V.1.10 Lemma.** *If $n \in \omega$, then either $n = \emptyset$ or $n = m \cup \{m\}$ for some $m \in \omega$.*

*Proof.* Let[‡] $\mathscr{P}(n) \equiv n = \emptyset \vee (\exists m \in \omega)(n = m \cup \{m\})$. Clearly, $\vdash \mathscr{P}(\emptyset)$, in pure logic, by axiom $x = x$ and substitution. Assume next $\mathscr{P}(x)$ for frozen $x$ (I.H.), and prove $\mathscr{P}(x \cup \{x\})$:

Now $\mathscr{P}(x)$ entails two cases, $x = \emptyset$ and $\neg x = \emptyset$. The first yields that $x \in \omega$. The second allows the introduction of the assumption

$$m \in \omega \wedge x = m \cup \{m\}$$

where $m$ is a new constant. Since $\omega$ is inductive, $x \in \omega$. Thus, the logical fact

$$\vdash x \cup \{x\} = x \cup \{x\}$$

and the substitution axiom **Ax2** yield

$$\vdash (\exists m)(m \in \omega \wedge x \cup \{x\} = m \cup \{m\})$$

and therefore $\vdash \mathscr{P}(x \cup \{x\})$ by tautological implication. □

**V.1.11 Definition (Transitive Classes).** A class $\mathbb{A}$ is *transitive* iff $x \in y \in \mathbb{A}$ implies $x \in \mathbb{A}$ for all $x, y$. □

[†] **ROB** stands for Robinson's axiomatic arithmetic, studied in volume 1, Chapter I.

[‡] "$\equiv$" means string equality (cf. I.1.4, p. 13).

This concept was introduced, in passing, in a footnote of Chapter IV. It is of the utmost importance: not only are the ordinals (in particular the formal natural numbers) transitive sets – while the class of all ordinals is a transitive class – but also such sets play a major role in the model theory of set theory.

Note that a class $\mathbb{A}$ is transitive amounts to $\mathrm{ran}(\in \restriction \mathbb{A}) \subseteq \mathbb{A}$, where, of course, we employ the symbol "$\in$" to denote the *relation* – $\{\langle y, x\rangle : x \in y\}$ – defined by the *nonlogical symbol* (predicate) also denoted "$\in$". In words: For all inputs $x \in \mathbb{A}$, the relation $\in$ has all its outputs in $\mathbb{A}$ as well. Or, as we say, $\mathbb{A}$ is $\in$-*closed.*[†]

**V.1.12 Lemma.** *Every natural number is a transitive set.*

*Proof.* We prove[‡]

$$(\forall z)(\forall x, y)(x \in y \in z \to x \in z) \tag{1}$$

by induction on $z$.

*Basis.* $x \in y \in \emptyset \to x \in \emptyset$ is provable, since $x \in y \in \emptyset$ is refutable.

*I.H.* For a frozen $z$ assume

$$(\forall x, y)(x \in y \in z \to x \in z) \tag{2}$$

Let now $x, y$ be frozen variables,[§] and add the assumption $x \in y \in z \cup \{z\}$.

*Case* $y \in z$. Then (I.H. and specialization) $x \in z \subseteq z \cup \{z\}$.
*Case* $y = z$. Then $x \in z \subseteq z \cup \{z\}$. By the deduction theorem,

$$x \in y \in z \cup \{z\} \to x \in z \cup \{z\}$$

Hence

$$(\forall x, y)(x \in y \in z \cup \{z\} \to x \in z \cup \{z\}) \qquad \square$$

**V.1.13 Lemma.** *$\omega$ is a transitive set.*

*Proof.* We prove

$$(\forall y)(\forall x)(x \in y \in \omega \to x \in \omega) \tag{1}$$

by induction on $y$.

[†] The reader will recall that in "$y \in x$", "$x$" is the input, for according to our conventions $\langle x, y\rangle$ is a pair in $\in$. A sizable part of the literature has "$y \in x$" to mean $\langle y, x\rangle$ is in $\in$, i.e., it has $y$ as the input. Naturally, for them, a transitive class is *not* $\in$-closed; instead it is $\in^{-1}$-closed.

[‡] We use the shorthand "$(\forall x, y)$" for "$(\forall x)(\forall y)$"

[§] That is, we must remember not to universally quantify them or substitute into them *prior* to our intended application of the deduction theorem.

*Basis.* $x \in \emptyset \in \omega \to x \in \omega$ is provable, since $x \in \emptyset \in \omega$ is refutable.

*I.H.* Freeze $y \in \omega$, and assume

$$(\forall x)(x \in y \in \omega \to x \in \omega) \tag{2}$$

To argue the case for $y \cup \{y\}$, let now $x$ be frozen[†] and add the assumption $x \in y \cup \{y\}$.

*Case* $x \in y$. Then (I.H. and specialization) $x \in \omega$.
*Case* $x = y$. Then $x \in \omega$.
Thus, we have proved (deduction theorem followed by generalization)

$$(\forall x)(x \in y \cup \{y\} \in \omega \to x \in \omega) \qquad \square$$

The above two lemmata say quite a bit about the structure of natural numbers:

(1) Every natural number is a transitive set.
(2) Every *member* of a natural number is a natural number (V.1.13).

Add to this that

(3) A natural number is a successor, or equal to $\emptyset$ (V.1.10),

and we have a complete characterization of natural numbers that does not need the axiom of infinity anymore. (See Exercise V.5.) Well, we will need infinity sooner or later, and we will need induction and inductive definitions over $\omega$ sooner rather than later, so it was not a bad idea to introduce the "whole" $\omega$ now.

**V.1.14 Example.** Is $\omega$ a successor? No, for if $\omega = x \cup \{x\}$ for some $x$, then $x \in \omega$. Since $\omega$ is inductive, $x \cup \{x\} \in \omega$ as well, i.e., $\omega \in \omega$, which is impossible by foundation. □

**V.1.15 Example (Predecessors).** By Lemmata V.1.8, V.1.9, and V.1.10 the formula $n \in \omega \to (\exists! m \in \omega)(n = \emptyset \wedge m = \emptyset \vee n \neq \emptyset \wedge n = m \cup \{m\})$ is provable in set theory.

Thus we can introduce a function symbol of arity 1, *pr*, the *predecessor function symbol*, by the axiom (see III.2.4, p. 122, in particular, (10), (11),

[†] In *argot* one often says "let $x$ be arbitrary but fixed", referring to the "value" of $x$.

(19), (20))

$$\begin{aligned} pr(x) = y \leftrightarrow \\ &\Big(x \in \omega \wedge (x = \emptyset \wedge y = \emptyset \vee x \neq \emptyset \wedge x = y \cup \{y\})\Big) \\ &\quad \vee x \notin \omega \wedge y = \emptyset \end{aligned} \tag{1}$$

Thus (aforementioned (19) and (20) respectively)

$$\vdash x \in \omega \rightarrow x = \emptyset \wedge pr(x) = \emptyset \vee x \neq \emptyset \wedge x = pr(x) \cup \{pr(x)\}$$

and

$$\vdash x \notin \omega \rightarrow pr(x) = \emptyset \qquad \square$$

**V.1.16 Remark.** By the above, whenever $n \neq \emptyset$ is a natural number, then its predecessor $pr(n)$ is also a natural number such that $pr(n) \in n$. By the transitivity of each natural number $n$, the predecessor of the predecessor of $n$ (if the latter is not $\emptyset$) is also a member of $n$, and so on; thus each natural number $n$ is the set of all natural numbers that "precede it" in the sense that "$m$ precedes $n$ iff $m \in n$".

This remark is important, yet trivial. Another way to see it is to note that $n = \{x : x \in n\}$ is provable for any set $n$. Now if $n \in \omega$, then so are all the $x \in n$, so with the notational convention of Definition V.1.5 one can write $n = \{m : m \in n\}$. □

**V.1.17 Theorem (The Minimality Principle for $\omega$, and for Any $n \in \omega$).**

(1) *For $\omega$: If $A$ is a nonempty subset of $\omega$, then there is an $m \in A$ such that $\neg(\exists n \in A)n \in m$.*
(2) *For any natural number $k$: If $A$ is a nonempty subset of $k$, then there is an $m \in A$ such that $\neg(\exists n \in A)n \in m$.*

An element such as $m$ is called an $\in$-minimal element of $A$.

*Proof.* (1): Formally, we want to prove the theorem schema

$$(\exists m)\mathscr{P}[m] \rightarrow (\exists m)\Big(\mathscr{P}[m] \wedge \neg(\exists n)\big(\mathscr{P}[n] \wedge n \in m\big)\Big)$$

By the *argot* conventions of V.1.5, the above is short for

$$(\exists x)(x \in \omega \wedge \mathscr{P}[x]) \rightarrow (\exists x)\Big(x \in \omega \wedge \mathscr{P}[x] \wedge \neg(\exists y)\big(y \in \omega \wedge \mathscr{P}[y] \wedge y \in x\big)\Big)$$

which is provable (for any $\mathscr{P}$) by the axiom of foundation.

(2): Formally, since $x \in k \leftrightarrow x \in \omega \wedge x \in k$ is provable by V.1.13, we just want to prove the theorem schema

$$(\exists m \in k)\mathscr{P}[m] \rightarrow (\exists m \in k)\Big(\mathscr{P}[m] \wedge \neg(\exists n \in k)\big(\mathscr{P}[n] \wedge n \in m\big)\Big)$$

This translates to

$$(\exists m)(m \in k \wedge \mathscr{P}[m]) \rightarrow (\exists m)\Big(m \in k \wedge \mathscr{P}[m] \wedge \neg(\exists n)\big(n \in k \wedge \mathscr{P}[n] \wedge n \in m\big)\Big)$$

and is provable by part (1). □

**V.1.18 Metatheorem (Relating $\omega$ and $\mathbb{N}$).** *There is a 1-1 correspondence $I : \mathbb{N} \rightarrow \omega$ – where "$\omega$" here denotes the "real" smallest inductive set – that* "translates the successor on $\mathbb{N}$ to the successor on $\omega$"*, namely,*

$$I(0) = \emptyset$$

*and, for $n \geq 0$, $n \in \mathbb{N}$,*

$$I(n + 1) = I(n) \cup \{I(n)\}$$

*Proof.* (*In the metatheory.*) Taking recursive (inductive) definitions over $\mathbb{N}$ for granted,[†] a unique and *total* $I$, as defined by recursion in the statement of the metatheorem, exists. Let us prove its other stated properties.

*1-1-ness:* By (metatheoretical) induction on $n - m \geq 1$ ($n, m$ in $\mathbb{N}$) over $\mathbb{N}$ we will prove that $m < n \rightarrow I(m) \in I(n)$, hence $m \neq n \rightarrow I(n) \neq I(m)$.

*Basis.* If $n - m = 1$, then $I(n) = I(m) \cup \{I(m)\}$.

*I.H.* Assume the claim for $n - m = k$. Case $n - m = k + 1$: Now $I(n) = I(m + k + 1)$, so that $I(m + k) \in I(n)$. By I.H., $I(m) \in I(m + k)$ so that $I(m) \in I(n)$, since the sets $I(i)$ are transitive.

*Ontoness:* By contradiction, let $n \in \omega$ be $\in$-minimal such that $n \notin \mathrm{ran}(I)$.[‡] Now, $n \neq \emptyset$ for $\emptyset \in \mathrm{ran}(I)$. Thus (V.1.15), $n = pr(n) \cup \{pr(n)\}$. Since $pr(n) \in n$ and $n$ is minimal with the above property, $pr(n)$ fails the property, that is, $pr(n) = I(m)$ for some $m \in \mathbb{N}$. But then $I(m + 1) = n$, hence $n \in \mathrm{ran}(I)$; a contradiction. □

**V.1.19 Remark.** In Metatheorem V.1.18 we have established that the "*real*" structures $(\mathbb{N}; 0, \lambda x.x + 1; <)$ and $(\omega; \emptyset, \lambda x.x \cup \{x\}; \in)$ are *isomorphic* in a

[†] See I.2.13, p. 26, for justification in a general setting. We will consider their formal counterparts over $\omega$ shortly.

[‡] By correctness and soundness of ZFC, the real $\omega$ satisfies the minimality principle, i.e., Theorem V.1.17 is really true.

unique (uniqueness of $I$) and "natural" way. This is the well-known result of naïve set theory that *the order type of* $\mathbb{N}$ *is* $\omega$.

(1) The isomorphism $I$ preserves the initial element ($I(0) = \emptyset$),
(2) it preserves the operation of successor ($I(n+1) = I(n) \cup \{I(n)\}$), *and*
(3) it preserves order (we proved above that $m < n \to I(m) \in I(n)$).
(4) $I$ uniquely *names* the formal natural numbers $\emptyset, \{\emptyset\}, \ldots$ as $0, 1, \ldots$; moreover,
(5) $I$, informally, assigns to each formal natural number its number of elements: It assigns 0 to $\emptyset$, which is correct, and if we assume that $n \in \mathbb{N}$ correctly measures the number of elements in $I(n)$ (induction over $\mathbb{N}$), then $n+1$ is the number of elements of $I(n) \cup \{I(n)\}$, for from $I(n) \notin I(n)$ it follows that $I(n)$ is a net new element added in passing from $I(n)$ to $I(n) \cup \{I(n)\}$.
(6) Further observing the "real" $\omega$ we extract one more piece of information: We know that $<$ on $\mathbb{N}$ satisfies *trichotomy*, i.e., for any $n, m$ in $\mathbb{N}$, $m < n \vee m = n \vee n < m$ is true. We know that $\in$ does not satisfy trichotomy on $\mathbb{U}_M$ (think of an example); however, in view of the isomorphism $I$, we expect that the transform of $<$ (that is, $\in$ *restricted to the real* $\omega$) does satisfy trichotomy. Indeed, *continuing to argue in the metatheory*, let $m, n$ be in $\omega$ such that $m \neq n$ and let $n', m'$ in $\mathbb{N}$ be such that $I(n') = n$, $I(m') = m$. By single-valuedness of $I$, $n' \neq m'$. Then $n' < m'$ or $m' < n'$; hence $n \in m$ or $m \in n$ respectively. So $(\forall m, n)(m \in n \vee m = n \vee n \in m)$ is true in (the real) $\omega$.

By Gödel's incompleteness theorem, there are really true sentences of the language of set theory that are not provable in ZFC. However, trichotomy

$$(\forall m, n)(m \in n \vee m = n \vee n \in m)$$

is not one of those. That this "truth" is formally provable *within set theory* we will see shortly. First, let us summarize our position vs. $\omega$:

☡☡ Hold on a minute! How do we *know* that trichotomy is true in $\mathbb{N}$? It positively is the wrong reason to advance that this might be because $\mathfrak{N}$, the standard model of **PA**, of course satisfies the **PA** axioms. That puts the cart well in advance of the horse, since the formal **PA** is an afterthought, a symbol-shuffling game we play within real mathematics. That is, we may rightly be accused here of circular thinking: **PA** proves trichotomy just because we *thought* trichotomy was *really* true, and so we "fixed" the **PA** axioms to derive it as a theorem!

Perhaps a more satisfying argument is that a real natural number indexes (counts) the members of a string of *strokes*, "|". Thus, if we have two natural numbers $m$ and $n$, we can associate with them two strings, $|\ldots|$ and $|\ldots|$, of the requisite numbers of strokes. We can think of such strings as the unary notations for those numbers.

Now, "obviously", if we superimpose the two sequences of strokes so that the two leftmost strokes in each coincide with each other, then either the two sequences totally coincide (case $m = n$), or the first sequence ends before the second (is a "prefix" of the second; case $m < n$), or the "otherwise" obtains ($m > n$). ☡☡

Metamathematically the two structures

$$(\mathbb{N}; 0, \lambda x . x + 1; <) \quad \text{and} \quad (\omega; \emptyset, \lambda x . x \cup \{x\}; \in)$$

are indistinguishable (which is pretty much what "isomorphic" means). This motivates the following behaviour on our part henceforth: From now on we will enrich the *argot* we speak when we do (formal) set theory to include:

"set of natural numbers" to mean $\omega$;
"natural number $n$" to mean $n \in \omega$

(that is, we drop the qualification "formal").

We will utilize the *naming* induced by the "external" (metamathematical) 1-1 correspondence $I$ without any further special notice, reserving the right to fall back to rigid notation ($\emptyset$,$\{\emptyset\}$, etc.) whenever we feel that the exposition will benefit from us doing so. Specifically, $n + 1$ stands for the successor $n \cup \{n\}$ in the context of natural numbers – in particular, we can write $n + 1 = n \cup \{n\}$.

$n - 1$ is another name for $pr(n)$ *whenever* $n \neq \emptyset$; we write 0 for $\emptyset$, 1 for $\{\emptyset\}$ and, in general, $n$ for $\{0, 1, \ldots, n - 1\}$ if $n \neq 0$.

We write $<$ for $\in$ whenever we feel that intuition will benefit from this notation. Then, $m \leq n$, i.e., $m < n \vee m = n$ is $m \in n \vee m = n$; in short, $m \subseteq n$ due to the transitivity of $n$.

In examples, and metamathematical discussions in general, we will continue to draw from our wider mathematical experience, and real sets such as $\mathbb{N}$ and $\mathbb{R}$ will continue being used and talked about. All we have done here is to find an *isomorphic image* of $\mathbb{N}$ in the real realm that is easily seen to have a formal counterpart within the formal theory. We are not saying that this (real $\omega$) is *really* the set of natural numbers rather than that ($\mathbb{N}$), as such a statement would be meaningless (and pointless) mathematically. It is the job of the philosopher to figure out exactly what *are* the natural numbers. The set theorist is content with using sets whose elements *behave like natural numbers* for purposes that include the ones articulated at the outset in this chapter. □

**V.1.20 Theorem (Trichotomy on $\omega$).**

$$\vdash_{\text{ZFC}} (\forall n)(\forall m)(m \in n \vee m = n \vee n \in m)$$

*Proof.* Recall V.1.5. We proceed by contradiction, so let us assume (or "add") instead

$$(\exists n)(\exists m)(\neg m \in n \wedge \neg m = n \wedge \neg n \in m) \tag{1}$$

By the minimality principle on $\omega$ (V.1.17), let $n_0$ be $\in$-minimal[†] in $\omega$ such that[‡]

$$(\exists m)(\neg m \in n_0 \wedge \neg m = n_0 \wedge \neg n_0 \in m) \tag{2}$$

Again, let $m_0$ be $\in$-minimal such that

$$\neg m_0 \in n_0 \wedge \neg m_0 = n_0 \wedge \neg n_0 \in m_0 \tag{3}$$

We proceed to prove $n_0 = m_0$, thus obtaining a contradiction.

Let $x \in n_0$ (which can also be written as "let $i \in n_0$" in view of V.1.13). By minimality of $n_0$, (2) yields $(\forall m)(m \in x \vee m = x \vee x \in m)$, and by specialization,

$$m_0 \in x \vee m_0 = x \vee x \in m_0 \tag{4}$$

Which $\vee$-clause is provable in (4)? Well, each of $m_0 \in x$ and $m_0 = x$ yields $m_0 \in n_0$ (using transitivity of $n_0$, V.1.12), which contradicts (3). It is then the case that $x \in m_0$, which proves $n_0 \subseteq m_0$.

The symmetry of (3) suggests (check it!) that an entirely analogous argument yields $x \in m_0 \to x \in n_0$ and hence $m_0 \subseteq n_0$. All in all, we have both (3) and $n_0 = m_0$, a contradiction. □

Because of trichotomy, $\in$-minimal elements in $\emptyset \neq A \subseteq \omega$ are unique, for if $m \neq n$ in $A$ are *both* $\in$-minimal, then we get the contradiction (to V.1.20)

$$\neg m \in n \wedge \neg n \in m \wedge \neg m = n$$

[†] The qualification "in $\omega$" can be omitted (indeed, it will be in the remainder of the proof) in view of the naming convention of V.1.5.

[‡] This uses proof by auxiliary constant, $n_0$, between the lines. The reader was forewarned at the beginning of Chapter IV that we will be increasingly using the "relaxed" proof style (see also III.5.9, p. 148).

An $\in$-minimal element $m$ of $A$ thus is also $\in$-*minimum* ($\in$-*least*, $\in$-*smallest*) or just *minimum* (*least*, *smallest*) in the sense that $x \in A \to m \in x \vee m = x$, or – to use our new *argot* – $x \in A \to m \leq x$. This is so by trichotomy, since $x \in m$ fails.

**V.1.21 Theorem (Recursive Definitions over $\omega$).** *Given a set $A$ and a total function $g : \omega \times A \to A$ in the sense of* III.11.12. *There exists a* unique *total function $f : \omega \to A$ that satisfies the following recursive definition:*

$$\begin{aligned} & f(0) = a, && \textit{where } a \in A \\ \textit{for } n \geq 0, \quad & f(n+1) = g(n, f(n)) && \end{aligned} \tag{$R$}$$

*Proof.* It is convenient to prove uniqueness first. Arguing by contradiction, let $f'$ satisfy the identical recursive definition as $f$ yet be different from $f$. Let $m$ be the least such that $f(m) \neq f'(m)$. By the basis of the definition $(R)$, $m \neq 0$, and hence $m - 1 \in \omega$ and $f(m-1) = f'(m-1)$. But then,

$$\begin{aligned} f(m) &= g(m-1, f(m-1)) \\ &= g(m-1, f'(m-1)) \\ &= f'(m) \end{aligned}$$

contradicting the hypothesis. Uniqueness is settled. Indeed, the argument applies unchanged for recursive definitions with a natural number $n$ as domain (i.e., total $f : n \to A$), since the minimality principle holds on $n$ as well (V.1.17).

We address existence next.

**Preamble.** For the existence part one is tempted to argue as follows:

**Argument.** $(R)$ gives the value of $f$ at 0, namely $a$. So, if we take the I.H. that $f(n)$ is defined, then $(R)$ (second equation) shows that $f(n+1)$ is also defined (since $g$ is total). By induction over $\omega$, $f$ is defined for all $n \in \omega$, hence it exists.

The above argument is drastically off the mark. All we really have argued about is that *any* $f$ that happens to satisfy $(R)$ also satisfies $\mathrm{dom}(f) = \omega$, or, "*if* an $f$ satisfying $(R)$ exists, then $\mathrm{dom}(f) = \omega$". Thus we have not proved existence at all. After all, a function $f$ does not need to be *total* in order to "exist".

The correct way to go about proving existence is to build "successive approximations" of $f$ by "finite" functions that satisfy $(R)$ on their domain. Each of these finite functions will have as domain some natural number $n \in \omega - \{0\}$. Towards this purpose we relax the "for $n \geq 0$" requirement in $(R)$. It turns out that these finite functions (if they exist) are pairwise consistent in that, for any two of them, $h$ and $p$, one has either $h \subseteq p$ or $p \subseteq h$. Thus the union of all of them is a function $f$. With a bit of extra work we show that $f$ is total and satisfies $(R)$.

Let

$$\begin{aligned}\mathscr{F} = \big\{ f : f \text{ is a function} \wedge \operatorname{dom}(f) \in \omega - \{0\} \wedge f(0) = a \wedge \\ (\forall k \in \operatorname{dom}(f))\big(k \neq 0 \to f(k) = g(k-1, f(k-1))\big)\big\}\end{aligned} \tag{1}$$

A fact used twice below is that $\mathscr{F} \neq \emptyset$. For example, $\{\langle 0, a\rangle\} \in \mathscr{F}$; also, $\{\langle 0, a\rangle, \langle 1, g(0, a)\rangle\} \in \mathscr{F}$. The first of these two functions has domain equal to 1, the second has domain equal to 2.

By the uniqueness part (applied to a function satisfying $(R)$ on domain $n$), for each $n \in \omega - \{0\}$ there is *at most one* $f \in \mathscr{F}$ with $\operatorname{dom}(f) = n$, hence, by collection (III.11.28), $\mathscr{F}$ is a set. So is then

$$\widehat{f} \stackrel{\text{def}}{=} \bigcup \mathscr{F} \tag{2}$$

Observe first that $\widehat{f}$ is a function: Let $\langle a, b\rangle \in \widehat{f}$ and also $\langle a, c\rangle \in \widehat{f}$. Then, by (2), $f(a) = b$ and $f'(a) = c$ for some $f$ and $f'$ in $\mathscr{F}$. Without loss of generality, applying trichotomy, $\operatorname{dom}(f) \in \operatorname{dom}(f')$.[†] By uniqueness, $f = f' \restriction \operatorname{dom}(f)$, since both sides of $=$ satisfy the same recurrence on $\operatorname{dom}(f)$.

Thus, $c = f'(a) = \big(f' \restriction \operatorname{dom}(f)\big)(a) = f(a) = b$, and therefore $\widehat{f}$ is single-valued.

We next argue that $\widehat{f}$ satisfies the recurrence: Trivially, $\widehat{f}(0) = a$ by $\{\langle 0, a\rangle\} \in \mathscr{F}$. Now

$$\begin{aligned}\widehat{f}(n+1) &= f(n+1) && \text{for some } f \in \mathscr{F} \\ &= g(n, f(n)) \\ &= g(n, \widehat{f}(n)) && \text{by } f \subseteq \widehat{f}\end{aligned}$$

We finally show that $\widehat{f}$ is total on $\omega$: Let instead $m$ be least such that $\widehat{f}(m) \uparrow$. Hence, $m \neq 0$ (since $\widehat{f}(0) \downarrow$, due to $\{\langle 0, a\rangle\} \in \mathscr{F}$) and $\widehat{f}(m-1) \downarrow$. Thus, $\widehat{f}(m-1) = f(m-1)$ for some $f \in \mathscr{F}$ with $\operatorname{dom}(f) = m$. Define $h : m+1, \to A$ by

$$h(x) = \begin{cases} f(x) & \text{if } x \in m \\ g(m-1, f(m-1)) & \text{if } x = m \end{cases}$$

Clearly $h \in \mathscr{F}(\operatorname{dom}(h) = m+1)$; thus $\widehat{f}(m) = h(m)$, a contradiction. □

[†] If $\operatorname{dom}(f) = \operatorname{dom}(f')$ then $f = f'$ by uniqueness, and hence $b = c$.

Although we have used trichotomy in the existence part, this can be avoided. See Exercise V.4.

We apply the theorem on recursive definitions to define addition on $\omega$.

**V.1.22 Definition (Addition of Natural Numbers).** Define $f_m : \omega \to \omega$ for each $m \in \omega$ by

$$\begin{aligned} f_m(0) &= m \\ f_m(n+1) &= f_m(n) + 1 \end{aligned} \qquad \square$$

**V.1.23 Remark.** Of course, for each $m$, $f_m$ is a set by separation ($f_m \subseteq \omega \times \omega$). The class

$$\{\langle \langle m, n \rangle, f_m(n) \rangle : \langle m, n \rangle \in \omega^2\} \tag{1}$$

is a set by collection (III.8.9). It is also single-valued in the second projection, for $\langle m, n \rangle = \langle m', n' \rangle$ implies $m = m'$, and hence (uniqueness – V.1.21) also $f_m = f_{m'}$. Finally, this implies $f_m(n) = f_{m'}(n')$, for our assumption yields $n = n'$, and the $f_m$ are functions.

We will call the set (1) "$+$", as tradition has it. That is, $+ : \omega \times \omega \to \omega$ satisfies (i.e., we can prove in ZFC) the following:

$$\begin{aligned} m + 0 &= m \\ m + (n+1) &= (m+n) + 1 \end{aligned}$$

In *form*, as it was dictated by intuition, the recursive definition of addition on $\omega$ is identical to the recursive definition of addition on $\mathbb{N}$ (only the interpretation of the nonlogical symbols changes). Naturally we expect addition on $\omega$ to enjoy the same properties as that over $\mathbb{N}$.

We note that the "$+$" just introduced is an *informal abbreviation* for a subset of $\omega^3$ (given by the set term (1) above) that also happens to be an important function. If we wish (we do not, however), we can also introduce a new *formal* function symbol, say, "$f_+$" by the explicit definition

$$f_+(x, y) = \begin{cases} x + y & \text{if } x \in \omega \wedge y \in \omega \\ \emptyset & \text{otherwise} \end{cases}$$

The reader will recall that we bow to the requirement that formal function symbols be total functions upon interpretation (e.g., over the standard model, which here has as underlying "set" the proper class $\mathbb{U}_M$). This is the reason for the "otherwise" part. Trivially,

$$\vdash_{\mathrm{ZFC}} x \in \omega \to f_+(x, 0) = x$$

and

$$\vdash_{\text{ZFC}} x \in \omega \to y \in \omega \to f_+\big(x, y \cup \{y\}\big) = f_+(x, y) \cup \{f_+(x, y)\} \qquad \Box$$

**V.1.24 Proposition (Commutativity of Addition).**

$$\vdash_{\text{ZFC}} (\forall n)(\forall m)(m + n = n + m)$$

*Proof.* We do induction on $n$.

*Basis.* $n = 0$. We want to prove

$$(\forall m)(m + 0 = 0 + m) \tag{2}$$

Anticipating success, this will also entail (by commutativity of equality and the Leibniz rule)

$$(\forall m)(0 + m = m + 0) \tag{2$'$}$$

Now $\vdash_{\text{ZFC}} (\forall m)(m + 0 = m)$ by V.1.23. It suffices to prove

$$(\forall m)(0 + m = m)$$

Regrettably, this requires an induction on $m$:

*Basis.* $m = 0$. That $\vdash_{\text{ZFC}} 0 + 0 = 0$ follows from V.1.23, which settles the basis (of the $m$-induction).

Let (I.H. on $m$) $0 + m = m$ for frozen $m$. Then (using "=" conjunctionally throughout this proof)

$$\begin{aligned} 0 + (m + 1) &= (0 + m) + 1 \qquad \text{by V.1.23} \\ &= m + 1 \qquad \text{by I.H. on } m \end{aligned}$$

This finally settles the basis (for $n$), namely, (2).

Assume now (I.H. on $n$) that

$$(\forall m)(m + n = n + m) \tag{3}$$

with frozen $n$. We embark on proving

$$(\forall m)(m + (n + 1) = (n + 1) + m) \tag{4}$$

We prove (4) by induction on $m$.

*Basis.* For $m = 0$ we want

$$0 + (n + 1) = (n + 1) + 0$$

which is provable by (2$'$) above via specialization.

We take now an I.H. on $m$, that is, we add the assumption

$$m + (n + 1) = (n + 1) + m \tag{5}$$

with frozen $m$ ($n$ was already frozen when we took assumption (3))

We embark on the final trip, i.e., to prove

$$(m + 1) + (n + 1) = (n + 1) + (m + 1)$$

Well,

$$\begin{aligned}
(n + 1) + (m + 1) &= ((n + 1) + m) + 1 && \text{by V.1.23}\\
&= (m + (n + 1)) + 1 && \text{by I.H. on } m \text{ (5)}\\
&= ((m + n) + 1) + 1 && \text{by V.1.23}\\
&= ((n + m) + 1) + 1 && \text{by I.H. on } n\text{: (3) and specialization}\\
&= (n + (m + 1)) + 1 && \text{by V.1.23}\\
&= ((m + 1) + n) + 1 && \text{by I.H. on } n\text{: (3) and specialization}\\
&= (m + 1) + (n + 1) && \text{by V.1.23}
\end{aligned}$$

(4) is now settled. □

The reader has just witnessed an application of the dreaded *double induction*. That is, to prove

$$(\forall n)(\forall m)\mathscr{P}(m, n) \tag{6}$$

one starts, in good faith, an induction on $n$. *En route* it turns out that in order to get unstuck one has to do an induction on $m$ as well, towards proving the basis $(\forall m)\mathscr{P}(m, 0)$ *and* the induction step $(\forall m)\mathscr{P}(m, n) \rightarrow (\forall m)\mathscr{P}(m, n + 1)$.

The good news is that it is not always necessary to do a double induction in order to prove something like (6). See for example the proof of the next result.

The reader can prove the *associativity* of $+$ (Exercise V.6), which we take for a fact from now on. Since, intuitively, $n = \{0, 1, \ldots, n-1\}$, then, intuitively, $n + m = \{0, 1, \ldots, n - 1, n + 0, n + 1, \ldots, n + (m - 1)\}$ . That is, to obtain $n + m$ we "concatenate" to the right of $n$ the elements of $m$ "shifted" by $n$. Formally this is true:

**V.1.25 Theorem.**

$$\vdash_{\mathrm{ZFC}} (\forall n)(\forall m)\Big(n + m = n \cup \{n + i : i \in m\}\Big)$$

*Proof.* By generalization, it suffices to prove

$$(\forall m)(n + m = n \cup \{n + i : i \in m\})$$

by induction on $m$.

*Basis.* For $m = 0$ (i.e., $m = \emptyset$) the claim amounts to $n + 0 = n \cup \emptyset$, while, trivially, $\vdash_{\text{ZFC}} n \cup \emptyset = n$. Done by V.1.23.

*I.H.* Assume

$$n + m = n \cup \{n + i : i \in m\}$$

for frozen $m$ and $n$. We look at the case $m + 1$: The left hand side is

$$\begin{aligned} n + (m + 1) &= (n + m) + 1 \qquad \text{by V.1.23} \\ &= (n + m) \cup \{n + m\} \qquad \text{(expanding “+1”)} \end{aligned} \tag{1}$$

The right-hand side is

$$\begin{aligned} n \cup \{n + i : i \in m \cup \{m\}\} &= n \cup \{n + i : i \in m\} \cup \{n + m\} \\ &= (n + m) \cup \{n + m\} \qquad \text{by I.H.} \end{aligned}$$

By (1), we are done. □

**V.1.26 Theorem.**

$$\vdash_{\text{ZFC}} (\forall n)(\forall m)\Big(n \le m \to (\exists! i) n + i = m\Big)$$

*Proof.* *Existence.* We argue by contradiction, so we add the assumption

$$(\exists n)(\exists m)\Big(n \le m \wedge \neg(\exists i) n + i = m\Big)$$

Let then – invoking proof by auxiliary constant between the lines, as in the proof of V.1.20 – $n_0$ be smallest such that[†]

$$(\exists m)\Big(n_0 \le m \wedge \neg(\exists i) n_0 + i = m\Big) \tag{1}$$

and next let $m_0$ be smallest such that

$$n_0 \le m_0 \wedge \neg(\exists i) n_0 + i = m_0 \tag{2}$$

[†] That is, “add the new constant $n_0$ and the assumption (1) along with $k < n_0 \to \neg(\exists m)\big(k \le m \wedge \neg(\exists i) k + i = m\big)$”.

Because of $\vdash_{\mathrm{ZFC}} n_0 + 0 = n_0$, (2) yields $\neg m_0 = n_0$: otherwise (i.e., adding the assumption $m_0 = n_0$) we get $\vdash_{\mathrm{ZFC}} n_0 + 0 = m_0$ and hence $\vdash_{\mathrm{ZFC}} (\exists i) n_0 + i = m_0$ by the substitution axiom (**Ax2**), contradicting (2).

Thus, from (2) (first conjunct, via V.1.19, p. 242), $\vdash_{\mathrm{ZFC}} n_0 \in m_0$; hence $\vdash_{\mathrm{ZFC}} m_0 \neq 0$. It follows that $m_0 = pr(m_0) \cup \{pr(m_0)\}$ (V.1.15); therefore $\vdash_{\mathrm{ZFC}} n_0 \leq m_0 - 1$ (V.1.19, p. 242). By minimality of $m_0$, there is an (auxiliary constant) $i$ such that $n_0 + i = m_0 - 1$; hence we have a ZFC proof of $m_0 = (n_0 + i) + 1 = n_0 + (i + 1)$ (employing "=" conjunctionally), contradicting the property (2) of $m_0$.

*Uniqueness*. Let $n_0$ be smallest such that

$$n_0 + i = n_0 + j \tag{3}$$

for some $i \neq j$. Now $n_0 \neq 0$, for $\vdash_{\mathrm{ZFC}} i = 0 + i$ and $\vdash_{\mathrm{ZFC}} 0 + j = j$ (V.1.24). Thus we can write (3) (using commutativity) as (i.e., we can prove)

$$(n_0 - 1) + i + 1 = (n_0 - 1) + j + 1$$

Since $i + 1 \neq j + 1$ (Lemma V.1.9), we have just contradicted the minimality of $n_0$. □

**V.1.27 Definition (Difference of Natural Numbers).** By V.1.26, the relation over $\omega$ below – which we denote by the *informal* symbol "–",

$$\{\langle\langle m, n\rangle, i\rangle : m = n + i\}$$

is single-valued in the second projection, that is, a *function*

$$- : \omega \to \omega$$

in the sense of III.11.12, called *difference*. By V.1.26,

$$\vdash_{\mathrm{ZFC}} n \leq m \to m - n \downarrow$$

and

$$\vdash_{\mathrm{ZFC}} n \leq m \to m = n + (m - n)$$

while

$$\vdash_{\mathrm{ZFC}} m < n \to m - n \uparrow$$ □

(1) We are painfully aware of the multiple meanings of the symbol "–" in set theory as set difference and, now, natural number difference, but such "overloading" of symbol meaning is common in mathematics.

(2) The difference between natural numbers does *not* coincide with the set difference of the two numbers. For example, in the former sense, $2 - 1 = 1 = \{0\}$, while in the latter sense $2 - 1 = \{0, 1\} - \{0\} = \{1\}$. The context will alert the reader if we (ever) perform $m - n$ in the "set sense" rather than the (normally) "natural number sense".

(3) Number difference is consistent with the earlier introduction of "$-$" in the context of predecessor. In the former sense, if $n \geq 1$, then $n-1$ is the unique number $m$ such that $m \cup \{m\} = n$, i.e., $m + 1 = n$; that $m$ is precisely the predecessor of $n$.

**V.1.28 Definition (Finite Sequences).** A *finite sequence* is a function $f$ such that $\mathrm{dom}(f) \in \omega$.

If $\mathrm{dom}(f) = 0$, then $f$ is the *empty sequence*. The *length* of the sequence $f$ is $\mathrm{dom}(f)$. If $i \in \mathrm{dom}(f)$, then $f(i)$ is the $i$th element of the sequence. □

Intuitively, a sequence $f$ is $[f(0), \ldots, f(n-1)]$ where $n = \mathrm{dom}(f) \neq 0$. If $\mathrm{dom}(f) = 0$, then we have the empty sequence $[\,]$.

We wish to distinguish between *vectors* and *finite sequences* although in a sense the two work the same way. They both give "order information" for a (finite) set. The technical differences are as follows:

(1) The vector $\langle a, b\rangle$ is the set $\{a, \{a, b\}\}$, while the sequence $[a, b]$ is the set $\{\langle 0, a\rangle, \langle 1, b\rangle\} = \big\{\{0, \{0, a\}\}, \{1, \{1, b\}\}\big\}$; thus they are different as sets.

(2) The vector $\langle x_1, \ldots, x_n\rangle$ has the *informal* $n$ in its *name*, so that $n$ cannot be manipulated by the formalism.[†] Thus $\langle x_1, \ldots, x_n\rangle$ is much like a set of unrelated variables $X1, \ldots, Xn$ in a programming language, while a sequence $f = \{\langle 0, x_1\rangle, \ldots, \langle n-1, x_n\rangle\}$ not only gives the same positional information, but also behaves like an array $f(i)$ for $i = 0, \ldots, n-1$ in a programming language; for the $i$ in $f(i)$ has formal status.

We often need to juxtapose or concatenate two sequences $f$ and $g$ to obtain $[f(0), \ldots, f(n-1), g(0), \ldots, g(m-1)]$ where $\mathrm{dom}(f) = n$, $\mathrm{dom}(g) = m$. Intuitively, the concatenation of $f$ and $g$, in that order, *is* a sequence, for we

[†] One can of course revisit the definition of $\langle \ldots \rangle$ and redefine it in terms of the formal numbers $n$. Such rewriting of history will be unwise in view of the commotion it will create. As it stands we are doing fine: The original definition allowed the theory to bootstrap itself up to a point where the present more general and more flexible definition of sequence was given.

can write it as $[f(0), \ldots, f(n-1), \widehat{g}(n+0), \ldots, \widehat{g}(n+(m-1))]$, where $\widehat{g}(n+i) = g(i)$ for all $i \in \mathrm{dom}(g)$ and undefined otherwise. That is, the concatenation is the function $f \cup \widehat{g}$.

**V.1.29 Definition (Concatenation of Finite Sequences).** If $f$ and $g$ are finite sequences, then the relation over $\omega$ given by

$$f \cup \{\langle \mathrm{dom}(f) + i, g(i)\rangle : i \in \mathrm{dom}(g)\}$$

– and denoted by $f * g$ – is called their *concatenation, in the order f followed by g*. □

**V.1.30 Proposition.** *For any two finite sequences $f$ and $g$, $f * g$ is a finite sequence of length* $\mathrm{dom}(f) + \mathrm{dom}(g)$.

*Proof.* Observe that $\mathrm{dom}(f) \subseteq \mathrm{dom}(f) + i$ (by V.1.25); hence $\mathrm{dom}(f) + i \notin \mathrm{dom}(f)$. In other words the domains of $f$ and $\{\langle \mathrm{dom}(f)+i, g(i)\rangle : i \in \mathrm{dom}(g)\}$ are disjoint.

Thus, $f * g$ *is* a function. Its domain, in view of the previous comment, is $\mathrm{dom}(f) \cup \{\mathrm{dom}(f) + i : i \in \mathrm{dom}(g)\}$, which is $\mathrm{dom}(f) + \mathrm{dom}(g)$ by V.1.25. □

**V.1.31 Corollary.** *If $f$ is the empty sequence and $g$ is some sequence, then $f * g = g * f = g$.*

☡ $f * g \neq g * f$ *in general*: Exercise V.10. ☡

**V.1.32 Proposition.** $\vdash_{\mathrm{ZFC}} \neg n < 0$.

*Proof.* That is, $\vdash_{\mathrm{ZFC}} \neg n \in \emptyset$. □

**V.1.33 Proposition.** $\vdash_{\mathrm{ZFC}} n < m + 1 \leftrightarrow n < m \vee n = m$.

*Proof.* That is, $\vdash_{\mathrm{ZFC}} n \in m \cup \{m\} \leftrightarrow n \in m \vee n = m$. □

Some more arithmetic over $\omega$ is delegated to the Exercises section.

☡☡ The reader who has read volume 1, Chapter II, now armed with V.1.8, V.1.9, V.1.23, Exercise V.11 (which introduces multiplication over $\omega$), V.1.20, V.1.32, and V.1.33 along with the induction principle over $\omega$, will see with a minimum of effort or imagination that *the Gödel incompleteness theorems hold for* ZFC – a fact that we took as a given in many earlier discussions.

Indeed, one need only carry out the *formal* Gödel numbering of volume 1, Chapter II, within ZFC (rather than within **PA**) using terms $t$ of ZFC that (provably) satisfy $t \in \omega$ as Gödel numbers of formulas, terms, and proofs in (any extension of) $L_{\mathrm{Set}}$. In this endeavour the proved results (for $\omega$) that we enumerated above – suggesting them as appropriate ammunition – play the role of **ROB** and induction, which – in arithmetic – were assumed axiomatically in volume 1.

Moreover, if $\Gamma$ denotes the set of individual ZFC axioms,[†] then it is easy to prove that the corresponding formula $\boldsymbol{\Gamma(x)}$ is recursive. Everything else has already been done in the aforementioned chapter.

## V.2. Algebra of Relations; Transitive Closure

**V.2.1 Informal Definition.** Let $\mathbb{P}$ and $\mathbb{S}$ be two relations. Then $\mathbb{P} \circ \mathbb{S}$, their *composition* in that order, is defined by

$$y\,\mathbb{P} \circ \mathbb{S}\,x \qquad \text{stands for} \qquad (\exists z)(y\,\mathbb{P}\,z \wedge z\,\mathbb{S}\,x)$$

or, equivalently,

$$y \in (\mathbb{P} \circ \mathbb{S})\langle x\rangle \qquad \text{abbreviates} \qquad \big(\exists z \in \mathbb{S}\langle x\rangle\big) y \in \mathbb{P}\langle z\rangle$$

We are adopting the notational convention that "$\mathbb{P} \circ \mathbb{S}\langle x\rangle$" means "$(\mathbb{P} \circ \mathbb{S})\langle x\rangle$", that is, we render the use of brackets redundant. □

**V.2.2 Remark.** Intuitively, $y \in \mathbb{P} \circ \mathbb{S}\langle x\rangle$ iff there is a "stepping stone", $z$, such that $\mathbb{S}$ sends $x$ to $z$ and $\mathbb{P}$ sends the latter to $y$.

If $\mathbb{S}$ is a *function*, then $y\,\mathbb{P}\,\mathbb{S}(x)$ (that is, $\langle \mathbb{S}(x), y\rangle \in \mathbb{P}$ – the reader may wish to review notational issues; see III.11.4 and III.11.14) means, by Definition III.11.16, $(\exists z)(z = \mathbb{S}(x) \wedge y\,\mathbb{P}\,z)$. This says the same thing as $y\,\mathbb{P} \circ \mathbb{S}\,x$ by Definition V.2.1 (remembering that $z = \mathbb{S}(x)$ iff $z\,\mathbb{S}\,x$ for functions – III.11.14). □

**V.2.3 Lemma.** *For any relations* $\mathbb{P}$ *and* $\mathbb{S}$ *and all* $x$, $\mathbb{P} \circ \mathbb{S}\langle x\rangle = \mathbb{P}[\mathbb{S}\langle x\rangle]$.

[†] Recall that separation and collection denote infinitely many axioms, and so does foundation in the form we have adopted, although the latter can be replaced by a single axiom.

*Proof.* $\subseteq$: Let $y \in \mathbb{P} \circ \mathbb{S}\langle x\rangle$. Then, for some $z$, $y \in \mathbb{P}\langle z\rangle \wedge z \in \mathbb{S}\langle x\rangle$.[†] That is, $y \in \mathbb{P}[\mathbb{S}\langle x\rangle]$ (Definition III.11.4).

$\supseteq$: Let $y \in \mathbb{P}[\mathbb{S}\langle x\rangle]$. Then, for some $z \in \mathbb{S}\langle x\rangle$, one has $y \in \mathbb{P}\langle z\rangle$; hence $y \in \mathbb{P} \circ \mathbb{S}\langle x\rangle$ by V.2.1. □

**V.2.4 Corollary.** *For any relations $\mathbb{P}$ and $\mathbb{S}$ and all $\mathbb{X}$, $\mathbb{P} \circ \mathbb{S}[\mathbb{X}] = \mathbb{P}\big[\mathbb{S}[\mathbb{X}]\big]$.*

Lemma V.2.3 justifies – at long last – the convention of writing "$y\,\mathbb{P}\,x$" for "$\langle x, y\rangle \in \mathbb{P}$".

Of course, the "standard" convention is to write instead $x\,\mathbb{P}\,y$, but it has a serious drawback: For functions $f$, $g$ *viewed as special cases of relations* – thus using *notation acceptable for relations* – $x\ f \circ g\ y$ would mean that $x$ is input for $f$ whose output is input to $g$; the latter yields $y$. In short, $y = g(f(x))$. "Standard" notation goes a step further to write $y = g \circ f(x)$, thus introducing the well-known (from elementary discrete mathematics texts) "reversal" from $f \circ g$ (when we are composing $f$ and $g$ "viewed as relations") to $g \circ f$ (when we are composing $f$ and $g$ "viewed as functions").

On the other hand, at the cost of being a bit unconventional at the outset, when $y\,\mathbb{P}\,x$ was defined, we proposed a convention that holds *uniformly* for relations *and* functions when it comes to composition. This (by Lemma V.2.3) says "in $y\,\mathbb{P} \circ \mathbb{S}\,x$, $\mathbb{S}$ acts first, on input $x$; one of its outputs, if it is inputed to $\mathbb{P}$, will cause output (possibly among other things) $y$".

**V.2.5 Example.** Let $R = \{\langle 1, 2\rangle, \langle 1, 3\rangle\}$ and $S = \{\langle 1, 1\rangle, \langle 2, 1\rangle\}$. Then

$$\begin{array}{lll} x S \circ R y & \text{iff} & (\exists z)(x S z \wedge z R y) \\ & \text{iff} & (\exists z)(\langle y, z\rangle \in R \wedge \langle z, x\rangle \in S) \end{array}$$

Thus $S \circ R = \{\langle 1, 1\rangle\}$. On the other hand, one similarly calculates that $R \circ S = \{\langle 1, 2\rangle, \langle 1, 3\rangle, \langle 2, 2\rangle, \langle 2, 3\rangle\}$.

Therefore, *in general*, $\nvdash_{\text{ZFC}} S \circ R = R \circ S$. □

**V.2.6 Lemma.** *For any relations $\mathbb{P}$, $\mathbb{S}$, $\mathbb{T}$*

$$\mathbb{P} \circ (\mathbb{S} \circ \mathbb{T}) = (\mathbb{P} \circ \mathbb{S}) \circ \mathbb{T}$$

*that is, composition is* associative.

[†] The reader who may long for the earlier tediously formal proof style will note that "$z$" can be thought of as the name of an auxiliary constant here.

**Digression.** By the (informal) definition of class equality (cf. III.4.7 and III.4.8) and the deduction theorem, a formula $\mathbb{A} = \mathbb{B}$ is proved by "letting $x \in \mathbb{A}$" (frozen $x$) and then proving $x \in \mathbb{B}$ to settle "$\subseteq$", subsequently repeating these steps with the roles of $\mathbb{A}$ and $\mathbb{B}$ reversed. We have already employed this technique in the proof of V.2.3.

When we deal with relations $\mathbb{P}$ and $\mathbb{S}$ and we want to prove $\mathbb{P} = \mathbb{S}$, the above technique translates to "letting" $x\,\mathbb{P}\,y$ in the "$\subseteq$-direction". The reason is that one really "lets"

$$z \in \mathbb{P} \tag{1}$$

Then (cf. III.11.1), $OP(z)$ follows, that is,

$$(\exists u)(\exists v)\langle u, v\rangle = z \tag{2}$$

Letting now $x$ and $y$ be auxiliary (new) constants, we can add the assumption $\langle y, x\rangle = z$ so that (1) becomes

$$x\,\mathbb{P}\,y \tag{3}$$

With some work, one then proves $x\,\mathbb{S}\,y$, that is, $z \in \mathbb{S}$. This settles $\mathbb{P} \subseteq \mathbb{S}$.

Thus, *in practice*, one is indeed justified in suppressing the steps (1)–(2) and start by "letting" (3).

*Proof.* $\subseteq$: Let $x\mathbb{P} \circ (\mathbb{S} \circ \mathbb{T})y$. Then (by V.2.1)

$$(\exists z)(x\,\mathbb{P}\,z \wedge z(\mathbb{S} \circ \mathbb{T})y)$$

Hence (by V.2.1)

$$(\exists z)\big(x\,\mathbb{P}\,z \wedge (\exists w)(z\,\mathbb{S}\,w \wedge w\,\mathbb{T}\,y)\big)$$

Hence ($w$ is not free in $x\,\mathbb{P}\,z$)

$$(\exists w)(\exists z)(x\,\mathbb{P}\,z \wedge z\,\mathbb{S}\,w \wedge w\,\mathbb{T}\,y)$$

Hence ($z$ is not free in $w\,\mathbb{T}\,y$)

$$(\exists w)\big((\exists z)(x\,\mathbb{P}\,z \wedge z\,\mathbb{S}\,w) \wedge w\,\mathbb{T}\,y\big)$$

Hence (by V.2.1)

$$(\exists w)\big((x\mathbb{P} \circ \mathbb{S}w) \wedge w\,\mathbb{T}\,y\big)$$

Hence (by V.2.1)

$$x(\mathbb{P} \circ \mathbb{S}) \circ \mathbb{T}y$$

The case for $\supseteq$ is entirely analogous. □

In view of the associativity of $\circ$, brackets are redundant in a chain of compositions involving the same relation $\mathbb{P}$. In particular,

$$\underbrace{\mathbb{P}\circ\cdots\circ\mathbb{P}}_{n \text{ copies}}$$

depends *only* on $\mathbb{P}$ and the number of copies, $n$. It should be naturally denoted by $\mathbb{P}^n$. Here we have been thinking in informal (metamathematical) terms, i.e., $n \in \mathbb{N}$.

We can say the same thing by an informal inductive definition (over $\mathbb{N}$):

**V.2.7 Tentative Definition ("Positive" Powers of a Relation).** Let $\mathbb{P}$ be any relation. Then

$$\begin{aligned} \mathbb{P}^1 &\overset{\text{def}}{=} \mathbb{P} \\ \mathbb{P}^{n+1} &\overset{\text{def}}{=} \mathbb{P}^n \circ \mathbb{P} \quad \text{for any } n \in \mathbb{N} \text{ such that } n > 0 \end{aligned} \qquad \square$$

This tentative definition is acceptable, but it has the drawback that it hides $n$ in the name, as we have already discussed in the preamble of Section V.1. We can fix this easily, *if* $\mathbb{P}$ *is a set*, by making V.2.7 into a formal recursive definition of a function $n \mapsto \mathbb{P}^n$ on $\omega$,[†] replacing "$n \in \mathbb{N}$" by "$n \in \omega$".[‡]

However we want to afford our exposition the generality that $\mathbb{P}$ may be a proper class. Intuitively, $x\,\mathbb{P}^n\,y$ ($n \in \omega$ and $n \neq 0$) should mean that for some sequence $[f_0, f_1, \ldots, f_n]$,

$$f_0\,\mathbb{P}\,f_1\,\mathbb{P}\cdots\mathbb{P}\,f_{n-1}\,\mathbb{P}\,f_n$$

where $x = f_0$ and $y = f_n$.

**V.2.8 Definition ("Positive" Powers of a Relation).** For any relation $\mathbb{P}$ (possibly a proper class), and any $n \in \omega - \{0\}$, the relation $\mathbb{P}^n$ is defined by

$$\begin{aligned} x\,\mathbb{P}^n\,y \quad \text{abbreviates} \quad & n \in \omega - \{0\} \wedge (\exists f)\big(f \text{ is a function} \wedge \operatorname{dom}(f) = n+1 \wedge \\ & f(0) = x \wedge f(n) = y \wedge (\forall j)(j < n \to f(j)\,\mathbb{P}\,f(j+1))\big) \end{aligned}$$

$\square$

The reader already knows how to express "$f$ is a function" within set theory.

[†] Technically, we then also need a meaning for $\mathbb{P}^0$, i.e., a value of the defined function at 0. As such we can take, for example, $\{\langle x, x\rangle : x \in \text{field}(\mathbb{P})\}$.

[‡] The requirement that $\mathbb{P}$ be a set makes the pairs $\langle n, \mathbb{P}^n\rangle$ of the recursively defined function meaningful, for the two components of a pair must be sets or atoms.

**V.2.9 Definition (Relational Identity).** The *identity* or *diagonal* relation *on the class* $\mathbb{A}$ is $\mathbf{1}_{\mathbb{A}} : \mathbb{A} \to \mathbb{A}$ (also denoted $\mathbf{\Delta}_{\mathbb{A}} : \mathbb{A} \to \mathbb{A}$) given by $\mathbf{1}_{\mathbb{A}} = \{\langle x, x\rangle : x \in \mathbb{A}\}$. Thus, $\mathbf{1}_{\mathbb{A}}$ is a *total function* $\mathbb{A} \to \mathbb{A}$.

If $\mathbb{A}$ is understood, then we simply write $\mathbf{1}$ or $\mathbf{\Delta}$.[†]

For any $\mathbb{P} : \mathbb{A} \to \mathbb{A}$ we let $\mathbb{P}^0$ abbreviate $\mathbf{1}_{\mathbb{A}}$. □

Some people define $\mathbb{P}^0$ as $\{\langle x, x\rangle : x = x\}$, but we prefer to make $\mathbb{P}^0$ context-sensitive. We note that $\mathbb{P}^n$ for $n > 0$ does *not* depend on the context $\mathbb{A}$ in which $\mathbb{P}$ was given (as $\mathbb{P} : \mathbb{A} \to \mathbb{A}$).

Thus, if we have a relation $R$ on a set $A$, then $R^0$ is the set $\{\langle x, x\rangle : x \in A\}$ rather than the proper class $\{\langle x, x\rangle : x = x\}$.

**Pause.** Why is $\{\langle x, x\rangle : x = x\}$ a proper class?

**V.2.10 Example.** Let $A = \{1, 2, 3\}$. Then $\mathbf{1}_{\mathbb{A}} = \mathbf{\Delta}_{\mathbb{A}} = \{\langle 1, 1\rangle, \langle 2, 2\rangle, \langle 3, 3\rangle\}$. □

**V.2.11 Lemma.** *For each* $\mathbb{P} : \mathbb{A} \to \mathbb{A}$*, one has* $\mathbb{P} \circ \mathbf{\Delta} = \mathbf{\Delta} \circ \mathbb{P} = \mathbb{P}$.

*Proof.* We have

$$y \in \mathbb{P} \circ \mathbf{\Delta}\langle x\rangle$$

iff (Lemma V.2.3)

$$y \in \mathbb{P}[\mathbf{\Delta}\langle x\rangle]$$

iff (Definition V.2.9)

$$y \in \mathbb{P}[\{x\}]$$

iff

$$y \in \mathbb{P}\langle x\rangle$$

Thus $\mathbb{P} \circ \mathbf{\Delta} = \mathbb{P}$. Similarly, $\mathbf{\Delta} \circ \mathbb{P} = \mathbb{P}$. □

**V.2.12 Proposition.** *For any relation* $\mathbb{P}$*,*

$$\begin{aligned} \vdash_{\mathrm{ZFC}} \mathbb{P}^1 &= \mathbb{P} \\ \vdash_{\mathrm{ZFC}} \mathbb{P}^{n+1} &= \mathbb{P}^n \circ \mathbb{P} \quad \textit{for any } n \in \omega - \{0\} \end{aligned}$$

[†] The context will guard against confusing this $\mathbf{\Delta}$ with that of volume 1, Chapter II.

*Proof.* By V.2.8, $x\,\mathbb{P}^1 y$ abbreviates

$$\begin{aligned}(\exists f)\big(&f \text{ is a function} \wedge \operatorname{dom}(f) = 2 \wedge \\ &f(0) = x \wedge f(1) = y \wedge (\forall j)(j < 1 \to f(j)\,\mathbb{P}\,f(j+1)\big)\end{aligned} \tag{1}$$

Since $\vdash_{\mathrm{ZFC}} j < 1 \leftrightarrow j = 0$ (recall that "$j < 1$" means "$j \in \{\emptyset\}$"), the one point rule (I.6.2) yields at once that (1) is provably equivalent to the following:

$$\begin{aligned}(\exists f)\big(&f \text{ is a function } \wedge \operatorname{dom}(f) = 2 \wedge \\ &f(0) = x \wedge f(1) = y \wedge f(0)\,\mathbb{P}\,f(1)\big)\end{aligned} \tag{2}$$

(2), in turn, is provably equivalent to $x\,\mathbb{P}\,y$.

To see the truth of the last claim, in view of (2) we introduce a new constant $f_0$ and the assumption

$$\begin{aligned}&f_0 \text{ is a function} \wedge \operatorname{dom}(f_0) = 2 \wedge \\ &f_0(0) = x \wedge f_0(1) = y \wedge f_0(0)\,\mathbb{P}\,f_0(1)\end{aligned} \tag{3}$$

the last three conjuncts of which yield $x\,\mathbb{P}\,y$.

Conversely, assuming $x\,\mathbb{P}\,y$, we get trivially

$$\begin{aligned}&\{\langle 0, x\rangle, \langle 1, y\rangle\} \text{ is a function} \wedge \operatorname{dom}(\{\langle 0, x\rangle, \langle 1, y\rangle\}) = 2 \wedge \\ &x = x \wedge y = y \wedge x\,\mathbb{P}\,y\end{aligned} \tag{4}$$

which yields (2) by the substitution axiom **Ax2**. This settles $\mathbb{P}^1 = \mathbb{P}$.

Next, assume

$$n > 0 \tag{5}$$

and

$$x\,\mathbb{P}^{n+1}\,y \tag{6}$$

These imply (by V.2.8)

$$\begin{aligned}n > 0 \wedge (\exists f)\Big(&f \text{ is a function} \wedge \operatorname{dom}(f) = n + 2 \wedge \\ &f(0) = x \wedge f(n+1) = y \wedge (\forall j)\big(j < n+1 \to f(j)\,\mathbb{P}\,f(j+1)\big)\Big)\end{aligned} \tag{7}$$

Note that $x\,\mathbb{P}^{n+1}\,y$ (cf. V.2.8) contributes the redundant (by V.1.8; hence *not included* in (7)) conjunct $n + 1 > 0$. By V.1.33 and employing tautological equivalences, distributivity of $\forall$ over $\wedge$, and the one point rule, (7) is provably equivalent to

$$n > 0 \wedge (\exists f)\Big(f \text{ is a function} \wedge \operatorname{dom}(f) = n+2 \wedge f(0) = x \wedge f(n+1) \\ = y \wedge (\forall j)\big(j < n \rightarrow f(j)\,\mathbb{P}\,f(j+1)\big) \wedge f(n)\,\mathbb{P}\,f(n+1)\Big) \tag{8}$$

(8) allows the introduction of a new constant $h$ and of the accompanying assumption

$$\begin{array}{l} h \text{ is a function} \wedge \operatorname{dom}(h) = n+2 \wedge h(0) = x \wedge \\ (\forall j)\big(j < n \rightarrow h(j)\,\mathbb{P}\,h(j+1)\big) \wedge h(n)\,\mathbb{P}\,y \end{array} \tag{9}$$

or, setting $g = h \restriction (n+1)$ – which implies $g(n) = h(n)$ in particular –

$$\begin{array}{l} g \text{ is a function} \wedge \operatorname{dom}(g) = n+1 \wedge g(0) = x \wedge g(n) = h(n) \wedge \\ (\forall j)\big(j < n \rightarrow g(j)\,\mathbb{P}\,g(j+1)\big) \wedge h(n)\,\mathbb{P}\,y \end{array}$$

which, by (5) and the substitution axiom, yields $x\,\mathbb{P}^n\,h(n)\,\mathbb{P}\,y$. Hence $x\,\mathbb{P}^n \circ \mathbb{P}\,y$.

The reader will have no trouble establishing the converse. □

Proposition V.2.12 captures formally the essence of Tentative Definition V.2.7 for *any* $\mathbb{P}$ (even a proper class), avoiding the technical difficulty (indeed, impossibility) of *defining* a proper-class-valued function.

We observe that *for a relation* $\mathbb{P}$ *on* $\mathbb{A}$, Definition V.2.9 is in harmony with V.2.12 in the sense that

$$\begin{aligned} \mathbb{P}^{0+1} &= \mathbb{P}^1 \\ &= \mathbb{P} \qquad \text{by V.2.12} \end{aligned}$$

and

$$\begin{aligned} \mathbb{P}^0 \circ \mathbb{P} &= \boldsymbol{\Delta} \circ \mathbb{P} \\ &= \mathbb{P} \qquad \text{by V.2.11} \end{aligned}$$

so that in this case $\vdash_{\text{ZFC}} \mathbb{P}^{n+1} = \mathbb{P}^n \circ \mathbb{P}$ for $n \geq 0$.

**V.2.13 Lemma (The Laws of Exponents).** *For any* $\mathbb{P} : \mathbb{A} \rightarrow \mathbb{A}$ *and* $j, m$ *in* $\omega$,

(*a*) $\vdash_{\text{ZFC}} \mathbb{P}^j \circ \mathbb{P}^m = \mathbb{P}^{j+m}$
(*b*) $\vdash_{\text{ZFC}} (\mathbb{P}^m)^j = \mathbb{P}^{mj}$.[†]

[†] For multiplication of natural numbers see Exercise V.11.

In the statement of the lemma, as is the normal practice, we use "implied multiplication", i.e., "$mj$" means $m \cdot j$. We will also follow the standard convention that "$\cdot$" has smaller scope (or higher "priority") than "+", so that $m + nj$ means $m + (nj)$.

*Proof.* ($a$): Induction on $m$. The case $m = 0$ requires the provability of $\mathbb{P}^j \circ \mathbf{1} = \mathbb{P}^j$, which is indeed the case by Lemma V.2.11. Now for the case $m + 1$ via the $m$-case using "=" conjunctionally:

$$\begin{aligned}
\mathbb{P}^j \circ \mathbb{P}^{m+1} &= \mathbb{P}^j \circ (\mathbb{P}^m \circ \mathbb{P}) && \text{(by V.2.12)}\\
&= (\mathbb{P}^j \circ \mathbb{P}^m) \circ \mathbb{P} && \text{(by associativity)}\\
&= \mathbb{P}^{j+m} \circ \mathbb{P} && \text{(by I.H.)}\\
&= \mathbb{P}^{j+m+1} && \text{(by V.2.12)}
\end{aligned}$$

($b$): Induction on $j$. The case $j = 0$ requires that $(\mathbb{P}^m)^0 = \mathbb{P}^0$ (i.e., $\mathbf{1} = \mathbf{1}$). For the case $j + 1$, via the $j$-case,

$$\begin{aligned}
(\mathbb{P}^m)^{j+1} &= (\mathbb{P}^m)^j \circ \mathbb{P}^m && \text{(by Proposition V.2.12)}\\
&= \mathbb{P}^{mj} \circ \mathbb{P}^m && \text{(by I.H.)}\\
&= \mathbb{P}^{mj+m} && \text{(by case } (a))\\
&= \mathbb{P}^{m(j+1)} && \text{(by Exercise V.11)}
\end{aligned}$$

□

By V.2.13($a$), $\vdash_{\text{ZFC}} \mathbb{P}^j \circ \mathbb{P}^m = \mathbb{P}^m \circ \mathbb{P}^j$ for any $\mathbb{P} : \mathbb{A} \to \mathbb{A}$ and $j, m$ in $\omega$. That is, powers of a relation commute with respect to composition.

**V.2.14 Definition.** A relation $\mathbb{P}$ is

(a) *symmetric* iff for all $x, y$, $x \mathbb{P} y$ implies $y \mathbb{P} x$.
(b) *antisymmetric* iff for all $x, y$, $x \mathbb{P} y \wedge y \mathbb{P} x$ implies $x = y$.
(c) *transitive* iff for all $x, y, z$, $x \mathbb{P} y \wedge y \mathbb{P} z$ implies $x \mathbb{P} z$.
(d) *irreflexive* iff for all $x, y$, $x \mathbb{P} y$ implies $x \neq y$.
(e) *reflexive on* $\mathbb{A}$ iff $(\forall x \in \mathbb{A}) x \mathbb{P} x$. □

(1) It is clear that (a) above says more, namely "$\mathbb{P}$ is symmetric iff $x \mathbb{P} y \leftrightarrow y \mathbb{P} x$", for the names $x, y$ can be interchanged in the definition.
(2) All concepts except reflexivity depend only on the relation $\mathbb{P}$, while reflexivity is *relative to a class* $\mathbb{A}$. If $\mathbb{P} : \mathbb{A} \to \mathbb{A}$ and if it is reflexive *on* $\mathbb{A}$, we usually say just "reflexive".

Reflexivity on $\mathbb{A}$ clearly is tantamount to $\mathbf{\Delta}_{\mathbb{A}} \subseteq \mathbb{P}$.

**V.2.15 Example.** $\emptyset$ is all of (a)–(d). It satisfies (e) only on $\emptyset$. □

**V.2.16 Example.** $\mathbf{\Delta}_{\mathbb{A}} : \mathbb{A} \to \mathbb{A}$ is all of (a)–(c). It fails (d). It satisfies (e) on $\mathbb{A}$.

Two obvious examples of irreflexive relations are $\subset$ on classes and $<$ on $\omega$, or, in the real realm, $\mathbb{N}$.

**V.2.17 Example (Informal).** The congruence modulo $m$ on $\mathbb{Z}$ is defined for $m > 1$ ($m \in \mathbb{Z}$) by

$$a \equiv_m b \qquad \text{iff} \qquad m \mid a - b$$

where "$x \mid y$" means that $(\exists z)(x \cdot z = y)$.

In number theory, rather than "$\ldots \equiv_m \ldots$" one uses the "dismembered" symbol "$\ldots \equiv \ldots \pmod{m}$".

We verify that $\equiv_m : \mathbb{Z} \to \mathbb{Z}$ is reflexive, symmetric, and transitive but not antisymmetric.[†]

Indeed, $m \mid a - a$ for *all* $a \in \mathbb{Z}$, which settles reflexivity. $m \mid a - b \to m \mid b - a$ for all $a, b$ settles symmetry. For transitivity we start with $m \mid a - b$ and $m \mid b - c$, that is, $a - b = km$ and $b - c = rm$ for $k$ and $r$ in $\mathbb{Z}$. Thus, $a - c = (k + r)m$; therefore $a \equiv_m c$.

To see that antisymmetry fails, just consider the fact that while $0 \equiv_m m$ and $m \equiv_m 0$, still $0 \neq m$. □

**V.2.18 Example (Informal).** $\leq$: $\mathbb{N} \to \mathbb{N}$ ("less than or equal" relation) is reflexive, antisymmetric, and transitive, but *not* symmetric. For example, $3 \leq 4$ but $4 \not\leq 3$.[‡] □

**V.2.19 Example.** Let $R = \{\langle 1, 2\rangle, \langle 2, 1\rangle, \langle 2, 3\rangle, \langle 3, 2\rangle, \langle 1, 1\rangle, \langle 2, 2\rangle, \langle 3, 3\rangle\}$ on the set $\{1, 2, 3\}$. $R$ is reflexive and symmetric, but is *not* antisymmetric or transitive. □

**V.2.20 Proposition.** $\mathbb{P}$ *is symmetric iff* $\mathbb{P} = \mathbb{P}^{-1}$ (cf. III.11.4). $\mathbb{P}$ *is transitive iff* $\mathbb{P}^2 \subseteq \mathbb{P}$.

*Proof.* For *symmetry*: *If part.* Let $\mathbb{P} = \mathbb{P}^{-1}$ and $x \,\mathbb{P}\, y$. Then $x \,\mathbb{P}^{-1}\, y$ as well; therefore $y \,\mathbb{P}\, x$, so that $\mathbb{P}$ is symmetric.

*Only-if part.* $\subseteq$: Let $\mathbb{P}$ be symmetric and $x \,\mathbb{P}\, y$. It follows that $y \,\mathbb{P}\, x$; therefore $x \,\mathbb{P}^{-1}\, y$ (by the definition of $\mathbb{P}^{-1}$).

[†] It goes almost without saying that no relation can be irreflexive *and* reflexive on a nonempty class.

[‡] It is usual, whenever it is typographically elegant, to denote the negation of $\ldots \mathbb{P} \ldots$, i.e., $\neg \ldots \mathbb{P} \ldots$, by $\ldots \not\mathbb{P} \ldots$, for any relation $\mathbb{P}$.

This settles $\subseteq$. The case for $\supseteq$ is entirely analogous.

For *transitivity*: *If part*. Let $\mathbb{P}^2 \subseteq \mathbb{P}$ and $x \mathbin{\mathbb{P}} y \mathbin{\mathbb{P}} z$.[†] Thus (definition of "$\circ$") $x \mathbin{\mathbb{P}^2} z$; hence $x \mathbin{\mathbb{P}} z$, so that $\mathbb{P}$ is transitive.

*Only-if part.* Assume transitivity and let $x \mathbin{\mathbb{P}^2} y$. Thus (definition of "$\circ$") $x \mathbin{\mathbb{P}} z \mathbin{\mathbb{P}} y$ for some $z$ (auxiliary constant). By transitivity, $x \mathbin{\mathbb{P}} y$; hence $\mathbb{P}^2 \subseteq \mathbb{P}$. □

**V.2.21 Example.** For any relations $\mathbb{P}$ and $\mathbb{S}$, $\vdash_{\text{ZFC}} (\mathbb{P} \cup \mathbb{S})^{-1} = \mathbb{P}^{-1} \cup \mathbb{S}^{-1}$.

Indeed, let $\langle x, y\rangle \in (\mathbb{P} \cup \mathbb{S})^{-1}$. Then

$$\langle y, x\rangle \in \mathbb{P} \cup \mathbb{S}$$

Hence

$$\langle y, x\rangle \in \mathbb{P} \vee \langle y, x\rangle \in \mathbb{S}$$

Hence

$$\langle x, y\rangle \in \mathbb{P}^{-1} \vee \langle x, y\rangle \in \mathbb{S}^{-1}$$

Hence

$$\langle x, y\rangle \in \mathbb{P}^{-1} \cup \mathbb{S}^{-1}$$

This settles $\subseteq$. The argument can clearly be reversed to establish $\supseteq$. □

**V.2.22 Definition (Closures).** Given $\mathbb{P}$.

(1) The *reflexive closure* of $\mathbb{P}$ *with respect to* $\mathbb{A}$, $r_{\mathbb{A}}(\mathbb{P})$, is the $\subseteq$-smallest relation $\mathbb{S}$ that is reflexive on $\mathbb{A}$ such that $\mathbb{P} \subseteq \mathbb{S}$.

(2) The *symmetric closure* of $\mathbb{P}$, $s(\mathbb{P})$, is the $\subseteq$-smallest symmetric relation $\mathbb{S}$ such that $\mathbb{P} \subseteq \mathbb{S}$.

(3) The *transitive closure* of $\mathbb{P}$, $t(\mathbb{P})$, is the $\subseteq$-smallest transitive relation $\mathbb{S}$ such that $\mathbb{P} \subseteq \mathbb{S}$. The alternative notation $\mathbb{P}^+$ is often used to denote $t(\mathbb{P})$. □

"$\mathbb{S}$ is $\subseteq$-smallest such that $\mathscr{F}$ holds" means that if $\mathscr{F}$ holds also for $\mathbb{T}$, then $\mathbb{S} \subseteq \mathbb{T}$.

[†] In analogy with the conjunctional use of "$<$" in $x < y < z$, one often uses an arbitrary relation $\mathbb{P}$ conjunctionally, so that $x \mathbin{\mathbb{P}} y \mathbin{\mathbb{P}} z$ stands for $x \mathbin{\mathbb{P}} y \wedge y \mathbin{\mathbb{P}} z$.

In anticipation of the following lemma, we used “the” as opposed to “a” in Definition V.2.22.

**V.2.23 Lemma (Uniqueness of Closures).** *Let* $\mathbb{S}$, $\mathbb{T}$ *be two* $q$*-closures of* $\mathbb{P}$ *of the same type* ($q \in \{r_{\mathbb{A}}, s, t\}$). *Then* $\mathbb{S} = \mathbb{T}$.

*Proof.* Let $\mathbb{S}$ pose as a $q$-closure of $\mathbb{P}$. Then $\mathbb{S} \subseteq \mathbb{T}$.

Now let $\mathbb{T}$ pose as a $q$-closure of $\mathbb{P}$. Then $\mathbb{T} \subseteq \mathbb{S}$. Hence $\mathbb{S} = \mathbb{T}$. □

**V.2.24 Lemma (Existence of Closures).** *Given a class* $\mathbb{A}$ *and a relation* $\mathbb{P}$. *Then*

($a$) $r_{\mathbb{A}}(\mathbb{P}) = \mathbb{P} \cup \mathbf{\Delta}_{\mathbb{A}}$,
($b$) $s(\mathbb{P}) = \mathbb{P} \cup \mathbb{P}^{-1}$,
($c$) $\mathbb{P}^{+} = \bigcup_{i=1}^{\infty} \mathbb{P}^{i}$.

$\mathbb{P}^{+} = \bigcup_{i=1}^{\infty} \mathbb{P}^{i}$ is, of course, to be understood as an abbreviation of $x\, \mathbb{P}^{+}\, y \leftrightarrow (\exists i \in \omega)(i > 0 \wedge x\, \mathbb{P}^{i}\, y)$.

*Proof.* ($a$): $\mathbb{P} \subseteq \mathbb{P} \cup \mathbf{\Delta}_{\mathbb{A}}$, and $\mathbb{P} \cup \mathbf{\Delta}_{\mathbb{A}}$ is reflexive on $\mathbb{A}$. Let also $\mathbb{T}$ be reflexive on $\mathbb{A}$, and $\mathbb{P} \subseteq \mathbb{T}$. Reflexivity of $\mathbb{T}$ contributes $\mathbf{\Delta}_{\mathbb{A}} \subseteq \mathbb{T}$. Thus, $\mathbb{P} \cup \mathbf{\Delta}_{\mathbb{A}} \subseteq \mathbb{T}$.

So $\mathbb{P} \cup \mathbf{\Delta}_{\mathbb{A}}$ is $\subseteq$-smallest.

($b$): Trivially, $\mathbb{P} \subseteq \mathbb{P} \cup \mathbb{P}^{-1}$. By V.2.20 and V.2.21, $\mathbb{P} \cup \mathbb{P}^{-1}$ is symmetric and hence a candidate for $s$-closure. Let now $\mathbb{P} \subseteq \mathbb{T}$ where $\mathbb{T}$ is symmetric and hence $\mathbb{T} = \mathbb{T}^{-1}$. Thus $\mathbb{P}^{-1} \subseteq \mathbb{T}^{-1} = \mathbb{T}$, from which $\mathbb{P} \cup \mathbb{P}^{-1} \subseteq \mathbb{T}$. Done.

($c$): Now $\mathbb{P} \subseteq \bigcup_{i=1}^{\infty} \mathbb{P}^{i}$ by V.2.12.

Next, we argue that $\bigcup_{i=1}^{\infty} \mathbb{P}^{i}$ is transitive.

Let $x(\bigcup_{i=1}^{\infty} \mathbb{P}^{i})y$ and $y(\bigcup_{i=1}^{\infty} \mathbb{P}^{i})z$. That is, $x\, \mathbb{P}^{j}\, y$ and $y\, \mathbb{P}^{m} z$ for some (auxiliary constants, cf. remark prior to this proof) $j, m$ ($\geq 1$), from which follows (by V.2.13) $x\, \mathbb{P}^{j+m}\, z$; hence ($j + m \geq 1$ is provable, clearly) $x(\bigcup_{i=1}^{\infty} \mathbb{P}^{i})z$, which settles transitivity.

To establish $\bigcup_{i=1}^{\infty} \mathbb{P}^{i}$ as $\subseteq$-smallest, let $\mathbb{T}$ be transitive and $\mathbb{P} \subseteq \mathbb{T}$. We claim that $j > 0 \rightarrow \mathbb{P}^{j} \subseteq \mathbb{T}$. We do (formal, of course) induction on $j$:

*Basis.* For $j = 0$ the claim is vacuously satisfied, since then $0 < j$ is refutable.

We assume the claim for frozen $j$ and proceed to prove[†]

$$\mathbb{P}^{j+1} \subseteq \mathbb{T} \tag{1}$$

There are two cases:

*Case* $j+1=1$. Then we are done by $\vdash \mathbb{P}^1 = \mathbb{P}$ (V.2.12) and the assumption $\mathbb{P} \subseteq \mathbb{T}$.

*Case* $j+1>1$. Thus $\vdash j > 0$. Therefore we have a proof

$$\begin{array}{ll}
x\,\mathbb{P}^{j+1}\,y & \\
(\exists z)(x\,\mathbb{P}^{j}\,z \wedge z\,\mathbb{P}\,y) & \Big\langle \text{V.2.12} \Big\rangle \\
(\exists z)(x\,\mathbb{T}\,z \wedge z\,\mathbb{T}\,y) & \Big\langle \text{I.H. and assumption on } \mathbb{T} \Big\rangle \\
x\,\mathbb{T}\,y & \Big\langle \mathbb{T} \text{ is transitive} \Big\rangle
\end{array}$$

which proves the induction step. $\bigcup_{i=1}^{\infty} \mathbb{P}^i \subseteq \mathbb{T}$ follows at once. □

**V.2.25 Example.** Why does a class $\mathbb{A}$ fail to be transitive? Because some set $x \in \mathbb{A}$ has members that are *not* in $\mathbb{A}$. If we fix this deficiency – by adding to $\mathbb{A}$ the missing members – we will turn $\mathbb{A}$ into a transitive class. All we have to do is to iterate the following process, until no *new* elements can be added:

> Add to *the current iterate of* $\mathbb{A}$ – call this $\mathbb{A}_i$ – *all* those elements $y$, not already included, such that $y \in x \in \mathbb{A}_i$ for all choices of $x$.

So, if we add a $y$, then we must add also all the $z \in y$ that were not already included, and all the $w \in z \in y$ that were not already included, . . . . In short, we add an element $w$ just in case $w \in z \in y \in \cdots \in x \in \mathbb{A}$ for some $z, y, \ldots, x$. With the help of the transitive closure – and switching notation from "$\in$ the nonlogical symbol" to "$\in$, the relation $\{\langle x, y\rangle : y \in x\}$"[‡] – this is simply put as:

> "*Add* a $w$ just in case $w \in^+ x \wedge x \in \mathbb{A}$ for some $x$", or
> "*Add* to the *original* $\mathbb{A}$ the class $\in^+ [\mathbb{A}]$ – i.e., form $\mathbb{A} \cup \in^+ [\mathbb{A}]$."

It turns out that $\mathbb{A} \cup \in^+ [\mathbb{A}]$ is the $\subseteq$-smallest transitive class that has $\mathbb{A}$ as a subclass – that is, it extends $\mathbb{A}$ to a transitive class in the most economical way (see below). □

[†] $\vdash_{\mathrm{ZFC}}\ j+1>0$ anyway.

[‡] The rightmost "$\in$" is the nonlogical symbol.

**V.2.26 Informal Definition (Transitive Closure of a Class).** For any class $\mathbb{A}$, the informal symbol $TC(\mathbb{A})$, pronounced *the transitive closure of the class* $\mathbb{A}$, stands for (abbreviates) $\mathbb{A} \cup \in^+ [\mathbb{A}]$. □

**V.2.27 Proposition.**

(1) *$TC(\mathbb{A})$ is the $\subseteq$-smallest* transitive *class that has $\mathbb{A}$ as a subclass.*
(2) *If $\mathbb{A} \subseteq TC(\mathbb{B})$, then $TC(\mathbb{A}) \subseteq TC(\mathbb{B})$.*
(3) *If $A$ is a set, then so is $TC(A)$.*

*Proof.* (1): Trivially, $\mathbb{A} \subseteq TC(\mathbb{A})$. Next, let $x \in y \in TC(\mathbb{A})$.

*Case 1.* $y \in \mathbb{A}$. Then $x \in (\in [\mathbb{A}]) \subseteq (\in^+ [\mathbb{A}])$,[†] since[‡] $\in$ is a subclass of $\in^+$. Hence $x \in TC(\mathbb{A})$.

*Case 2.* $y \in \in^+ [\mathbb{A}]$. Say $y \in \in^i [\mathbb{A}]$ for some $i \in \omega - \{0\}$. Then $x \in \in [\in^i [\mathbb{A}]]$. Moreover, we have the following simple calculation, where we have used the leftmost predicates in each line conjunctionally.

$$\begin{aligned} x \in\ & \in [\in^i [\mathbb{A}]] \\ =\ & \in \circ \in^i [\mathbb{A}], && \text{by V.2.4} \\ =\ & \in^{i+1} [\mathbb{A}], && \text{by V.2.12} \\ \subseteq\ & \in^+ [\mathbb{A}] \\ \subseteq\ & TC(\mathbb{A}) \end{aligned}$$

Thus $TC(\mathbb{A})$ is transitive.

Finally, let $\mathbb{A} \subseteq \mathbb{B}$ and $\mathbb{B}$ be transitive. Let $x \in \in^+ [\mathbb{A}]$. As above, $x \in \in^i [\mathbb{A}]$ for some $i \in \omega - \{0\}$. We want to conclude that $x \in \mathbb{B}$. For variety's sake we argue by contradiction, so let $i_0 > 0$ (auxiliary constant) be smallest such that for some $x_0$ (auxiliary constant) the contention fails, that is, add

$$x_0 \in \in^{i_0} [\mathbb{A}] \wedge \neg x_0 \in \mathbb{B}$$

Now $i_0 \neq 1$ is provable, for, if we add $i_0 = 1$, then $x_0 \in \in^{i_0} [\mathbb{A}]$ means that $(\exists y)(x_0 \in y \in \mathbb{A})$; hence $(\exists y)(x_0 \in y \in \mathbb{B})$ by hypothesis. Thus, $x_0 \in \mathbb{B}$, since $\mathbb{B}$ is transitive, and we have just contradicted what we have assumed about membership of $x_0$ in $\mathbb{B}$.

Thus, $i = i_0 - 1 > 0$, and, by minimality of $i_0$,

$$(\forall y)(y \in \in^i [\mathbb{A}] \rightarrow y \in \mathbb{B}) \tag{$*$}$$

[†] Brackets are inserted this once for the sake of clarity. They are omitted in the rest of the proof.

[‡] It is rather easy to see, from the context, when "$\in$" stands for the relation and when for the predicate.

Now

$$x_0 \in \in^{i_0} [\mathbb{A}] \to x_0 \in \in [\in^{i_0-1} [\mathbb{A}]], \qquad \text{by V.2.4}$$

Hence

$$x_0 \in y \in \in^{i} [\mathbb{A}] \qquad \text{for some } y$$

Therefore

$$x_0 \in y \in \mathbb{B}, \text{ by } (*)$$

and

$$x_0 \in \mathbb{B}, \qquad \text{since } \mathbb{B} \text{ is transitive.}$$

We have contradicted the choice of $i_0$ and $x_0$, and this settles (1).

(2) follows trivially from (1).

(3): For any class $\mathbb{T}$,

$$\in [\mathbb{T}] = \{x : (\exists y \in \mathbb{T}) x \in y\} = \bigcup \mathbb{T}$$

Thus, by induction on $i$, one can easily prove that $\in^i\ [A]$ is a set (having defined $\in^0\ [\mathbb{A}]$ to mean $\mathbb{A}$ for convenience), since

$$\in^{i+1} [A] = \in [\in^i\ [A]] = \bigcup \in^i\ [A]$$

Then, by collection (e.g., III.11.28),

$$S = \{A, \in [A], \in^2 [A], \ldots, \in^i\ [A], \ldots\}$$

is a set, and (by union) so is $TC(A) = \bigcup S$. □

From the above we infer that another way to "construct" $TC(\mathbb{A})$ is to throw in all the elements of $\mathbb{A}$, then all the elements of all the elements of $\mathbb{A}$, then all the elements of all the elements of all the elements of $\mathbb{A}$, and so on. That is, $TC(\mathbb{A}) = \mathbb{A} \cup \bigcup \mathbb{A} \cup \bigcup \bigcup \mathbb{A} \cup \bigcup \bigcup \bigcup \mathbb{A} \ldots$

**V.2.28 Remark.** (1) It follows from Lemma V.2.24 (if that were not already clear from the definition) that the $s$- and $t$-closures are *only* dependent on the relation we are closing, and not on any other context. On the contrary, the reflexive closure depends on a context $\mathbb{A}$.

(2) We also note that closing a relation $\mathbb{P}$ amounts, intuitively, to adding pairs $\langle x, y\rangle$ to $\mathbb{P}$ until the *first time* it acquires the desired property (reflexivity on some $\mathbb{A}$, or symmetry or transitivity). Correspondingly, $\mathbb{P}$ is reflexive on $\mathbb{A}$,

or symmetric or transitive, iff it equals its corresponding closure. This readily follows from the $\subseteq$-minimality of closures. □

**V.2.29 Example (Informal).** If $A = \{1, 2, \ldots, n\}$, $n \geq 1$, then $A \times A$ has $2^{n^2}$ subsets, that is, there are $2^{n^2}$ relations $P : A \to A$. Fix attention on one such relation, say, $R$.

Clearly then, the sequence $R, R^2, R^3, \ldots, R^i, \ldots$ has at most $2^{n^2}$ distinct terms, thus

$$R^+ = \bigcup_{i=1}^{2^{n^2}} R^i$$

With some extra work one can show that

$$R^+ = \bigcup_{i=1}^{n} R^i$$

in this case. Moreover, if $R$ is reflexive (on $A$, that is), then

$$R^+ = R^{n-1}$$ □

**V.2.30 Example.** Let the "higher order collection" of relations $(\mathbb{T}_a)_{a\in\mathbb{I}}$ be given by a formula of set theory, $\mathscr{T}(a, x, y)$, in the sense that

$$x \,\mathbb{T}_a\, y \qquad \text{abbreviates} \qquad \mathscr{T}(a, x, y)$$

so that $\bigcup_{a\in\mathbb{I}} \mathbb{T}_a$ stands for $\{\langle x, y\rangle : (\exists a \in \mathbb{I})\mathscr{T}(a, x, y)\}$. Let $\mathbb{S}$ be another relation.

Then the following two (abbreviations of) formulas are provable in ZFC:

$$\mathbb{S} \circ \left(\bigcup_{a\in\mathbb{I}} \mathbb{T}_a\right) = \bigcup_{a\in\mathbb{I}} (\mathbb{S} \circ \mathbb{T}_a) \tag{1}$$

$$\left(\bigcup_{a\in\mathbb{I}} \mathbb{T}_a\right) \circ \mathbb{S} = \bigcup_{a\in\mathbb{I}} (\mathbb{T}_a \circ \mathbb{S}) \tag{2}$$

We prove (1), leaving (2) as an exercise. Let

$$x \,\mathbb{S} \circ \left(\bigcup_{a\in\mathbb{I}} \mathbb{T}_a\right) y.$$

Then

$$(\exists z)\Big(x \,\mathbb{S}\, z \wedge z \left(\bigcup_{a\in\mathbb{I}} \mathbb{T}_a\right) y\Big)$$

Hence (via some trivial logical manipulations)

$$(\exists a \in \mathbb{I})(\exists z)(x\,\mathbb{S}\,z \wedge z\,\mathbb{T}_a\,y)$$

which yields

$$(\exists a \in \mathbb{I})(x\,\mathbb{S} \circ \mathbb{T}_a\,y)$$

and finally

$$x \bigcup_{a\in\mathbb{I}} (\mathbb{S} \circ \mathbb{T}_a)\,y$$

This settles $\subseteq$; the $\supseteq$-part is similar. □

**V.2.31 Example.** Consider now $\mathbb{P} : \mathbb{A} \to \mathbb{A}$. We will write $\mathbf{\Delta}$ for $\mathbf{\Delta}_{\mathbb{A}}$. We will show that

$$\vdash_{\mathrm{ZFC}} (\forall m)\Big((\mathbf{\Delta} \cup \mathbb{P})^m = \bigcup_{i=0}^{m} \mathbb{P}^i\Big) \tag{3}$$

We do induction on $m$. For $m = 0$, (3) requires $\vdash_{\mathrm{ZFC}} \mathbf{\Delta} = \mathbf{\Delta}$, a logical fact.

I.H.: Assume (3) for some fixed $m \geq 0$.

Case $m + 1$ (employing "$=$" conjunctionally):

$$\begin{aligned}
(\mathbf{\Delta} \cup \mathbb{P})^{m+1} &= \left(\bigcup_{i=0}^{m} \mathbb{P}^i\right) \circ (\mathbf{\Delta} \cup \mathbb{P}) \qquad \text{(by I.H.)}\\
&= \bigcup_{i=0}^{m} \big(\mathbb{P}^i \circ (\mathbf{\Delta} \cup \mathbb{P})\big) \qquad \text{(by V.2.30, case (2))}\\
&= \bigcup_{i=0}^{m} (\mathbb{P}^i \cup \mathbb{P}^{i+1}) \qquad \text{(by V.2.30, case (1), and V.2.11)}\\
&= \bigcup_{i=0}^{m+1} \mathbb{P}^i
\end{aligned}$$

As an application of this result, we look into $tr(\mathbb{P})$, or more correctly, $t\big(r(\mathbb{P})\big)$: the transitive closure of the reflexive closure of $\mathbb{P}$. We "calculate" as follows:

$$tr(\mathbb{P}) = t(\mathbf{\Delta} \cup \mathbb{P}) = \bigcup_{i=1}^{\infty} (\mathbf{\Delta} \cup \mathbb{P})^i = \bigcup_{i=1}^{\infty} \bigcup_{k=0}^{i} \mathbb{P}^k = \bigcup_{i=0}^{\infty} \mathbb{P}^i$$

Thus

$$tr(\mathbb{P}) = \bigcup_{i=0}^{\infty} \mathbb{P}^i \tag{4}$$

Next, look into $rt(\mathbb{P})$ (really $r\big(t(\mathbb{P})\big)$: the reflexive closure of the transitive closure of $\mathbb{P}$). Clearly,

$$rt(\mathbb{P}) = \mathbf{\Delta} \cup t(\mathbb{P}) = \bigcup_{i=0}^{\infty} \mathbb{P}^i \tag{5}$$

By (4) and (5), $\vdash_{\mathrm{ZFC}} rt(\mathbb{P}) = tr(\mathbb{P})$. We call this relation ($rt(\mathbb{P})$ or $tr(\mathbb{P})$) the *reflexive-transitive closure* of $\mathbb{P}$. It usually goes under the symbol $\mathbb{P}^*$. Thus, *intuitively*, $x\,\mathbb{P}^*\,y$ iff either $x = y$, or for some $z_1, \ldots, z_{k-1}$ for $k \geq 1$, $x\,\mathbb{P}\,z_1\,\mathbb{P}\,z_2 \ldots z_{k-1}\,\mathbb{P}\,y$.[†] □

**V.2.32 Informal Definition (Adjacency Map).** Given a relation $\mathbb{P} : \mathbb{A} \to \mathbb{B}$, its *adjacency map* $M_{\mathbb{P}}$ is

$$\big\{\langle\langle x, y\rangle, i\rangle : x \in \mathbb{A} \wedge y \in \mathbb{B} \wedge i \in \{0, 1\} \wedge (i = 1 \leftrightarrow \langle x, y\rangle \in \mathbb{P})\big\} \qquad \square$$

In applications the most interesting case of adjacency maps occurs when $\mathbb{A} = \mathbb{B} = \{a_0, \ldots, a_{n-1}\}$, a finite set of $n$ elements (we have, intuitively, $n$ elements iff $i \neq j \to a_i \neq a_j$).[‡] In this case we have relations $P$ on $A$, a set; therefore any such $P$ is a set too. The adjacency map $M_P$ can be represented, or "stored" (in a computer, for example), as a *table*, $A_P$, known as an *adjacency matrix*, via the definition

$$A_P(i, j) \overset{\text{def}}{=} M_P(\langle a_i, a_j\rangle)$$

that is, $A_P$ is $n \times n$ and

$$A_P(i, j) \overset{\text{def}}{=} \begin{cases} 1 & \text{if } \langle a_i, a_j\rangle \in P \\ 0 & \text{otherwise} \end{cases}$$

We understand $i$ as the row index and $j$ as the column index.

[†] For $k = 1$ the sequence $z_1, \ldots, z_{k-1}$ is empty by convention; thus we just have $x\,\mathbb{P}\,y$ in this case.

[‡] The $a_i$ can be thought of as values of a function $f$ with domain $n$, that is $a_i = f(i)$.

**V.2.33 Example (Informal).** Consider $R = \{\langle a, b\rangle, \langle b, c\rangle\}$ on $A = \{a, b, c\}$, where $a \neq b \neq c \neq a$. Let us arbitrarily rename $a$, $b$, $c$ as $a_1$, $a_2$, $a_3$ respectively – or, equivalently, 1, 2, 3, since the $a$ in $a_i$ is clearly cosmetic. Then,

$$A_R = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

$$A_{r(R)} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

$$A_{R^+} = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

$$A_{st(R)} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

$$A_{ts(R)} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

□

**V.2.34 Example (Informal).** Consider $\boldsymbol{\Delta} : S \to S$, where $S = \{1, 2, \ldots, n\}$. Then

$$A_{\Delta}(i, j) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

That is, $A_{\Delta}$ has 1's only on the main diagonal. This observation partly justifies the term "diagonal relation". □

**V.2.35 Example (Informal).** Given $R : A \to A$ and $S : A \to A$, where $A = \{a_1, a_2, \ldots, a_n\}$ and $a_i \neq a_j$ if $i \neq j$. We can form $R^{-1}$, $r(R)$, $s(R)$, $R^+$, $R^*$, $R \cup S$, $R \circ S$, $S \circ R$, etc. What are their adjacency matrices?

First, let us agree that *in the context of adjacency matrices* the operation "+" on {0, 1} is given by[†]

$$x + y = \begin{cases} 1 & \text{if } x + y \geq 1 \\ 0 & \text{otherwise} \end{cases}$$

[†] This "+" is often called *Boolean addition*, for if 0, 1 are thought of as the values *false* and *true* respectively, the operation amounts to "$\vee$".

Now, going from easy to hard:

(1) $A_{R^{-1}}$ satisfies $A_{R^{-1}}(i, j) = A_R(j, i)$ for all $i$, $j$, i.e., in matrix jargon, $A_{R^{-1}}$ is the *transpose* of $A_R$.

(2) $A_{R\cup S} = A_R + A_S$, that is, $A_{R\cup S}(i, j) = A_R(i, j) + A_S(i, j)$ for all $i$, $j$. We say that $A_{R\cup S}$ is the *Boolean sum* of $A_R$ and $A_S$.

(3) In particular, $A_{r(R)} = A_{\mathbf{\Delta}\cup R} = A_{\mathbf{\Delta}} + A_R$; thus we pass from $A_R$ to $A_{r(R)}$ by making all the diagonal entries equal to 1.

(4) $A_{s(R)} = A_{R\cup R^{-1}} = A_R + A_{R^{-1}}$, so that $A_{s(R)}(i, j) = A_R(i, j) + A_R(j, i)$ for all $i$, $j$.

(5) What is $A_{R\circ S}$ in terms of $A_R$, $A_S$? We have

$$\begin{aligned}
A_{R\circ S}(i, j) = 1 \quad &\text{iff} \quad \langle a_i, a_j\rangle \in R \circ S\\
&\text{iff} \quad a_j R \circ S a_i\\
&\text{iff} \quad (\exists m)(a_j R a_m \wedge a_m S a_i)\\
&\text{iff} \quad (\exists m)(\langle a_m, a_j\rangle \in R \wedge \langle a_i, a_m\rangle \in S)\\
&\text{iff} \quad (\exists m)(A_S(i, m) = 1 \wedge A_R(m, j) = 1)\\
&\text{iff} \quad \sum_{m=1}^{n} A_S(i, m) \cdot A_R(m, j) = 1\\
&\text{iff} \quad (A_S \cdot A_R)(i, j) = 1
\end{aligned}$$

Thus, $A_{R\circ S} = A_S \cdot A_R$ (note the order reversal!).

(6) In particular, $A_{R^{m+1}} = A_{R^m \circ R} = A_R \cdot A_{R^m}$. If now we assume inductively that $A_{R^m} = (A_R)^m$ (which is clearly true[†] for $m = 0$), then $A_{R^{m+1}} = (A_R)^{m+1}$. Thus $A_{R^m} = (A_R)^m$ is true for all $m \geq 0$.

(7) It follows from (2), (6), and Exercise V.23 that

$$A_{R^+} = \sum_{i=1}^{n} (A_R)^i$$

whereas

$$A_{R^*} = \sum_{i=0}^{n} (A_R)^i$$

From the observation that $R^* = tr(R)$ and from Exercise V.24 one gets

$$A_{R^*} = (A_{\mathbf{\Delta}} + A_R)^{n-1}$$

a simpler formula.

The reader will be asked to pursue this a bit more in the Exercises section, where "good" algorithms for the computation of $A_{R^+}$ and $A_{R^*}$ will be sought. □

[†] We did say that this example is in the informal domain.

## V.3. Algebra of Functions

**V.3.1 Definition.** Given functions $f : \mathbb{A} \to \mathbb{B}$ and $g : \mathbb{B} \to \mathbb{A}$ such that $g \circ f = \mathbf{\Delta}_{\mathbb{A}}$. We say that $g$ is *a left inverse* of $f$, and $f$ is *a right inverse* of $g$. □

**V.3.2 Remark.** We will follow in this section the convention of using $f, g, h$ and possibly other lowercase letters, with or without subscripts or primes, as *function names* even in those cases that the functions might be proper classes. We will continue utilizing uppercase letters for "general" relations. Any startling deviations from this notational rule will be noted. □

**V.3.3 Example (Informal).** Let $A = \{a, b\}$, where $a \neq b$, and $B = \{1, 2, 3, 4\}$. Consider the following functions:

$$\begin{aligned}
f_1 &= \{\langle a, 1\rangle, \langle b, 3\rangle\}\\
f_2 &= \{\langle a, 1\rangle, \langle b, 4\rangle\}\\
g_1 &= \{\langle 1, a\rangle, \langle 3, b\rangle, \langle 4, b\rangle\}\\
g_2 &= \{\langle 1, a\rangle, \langle 2, b\rangle, \langle 3, b\rangle\}\\
g_3 &= \{\langle 1, a\rangle, \langle 2, b\rangle, \langle 3, b\rangle, \langle 4, b\rangle\}\\
g_4 &= \{\langle 1, a\rangle, \langle 2, a\rangle, \langle 3, b\rangle, \langle 4, b\rangle\}\\
g_5 &= \{\langle 1, a\rangle, \langle 3, b\rangle\}
\end{aligned}$$

We observe that

$$\begin{aligned}
g_1 \circ f_1 &= g_2 \circ f_1 = g_3 \circ f_1 = g_4 \circ f_1 = g_5 \circ f_1 = g_1 \circ f_2 = g_3 \circ f_2\\
&= g_4 \circ f_2 = \mathbf{\Delta}_A
\end{aligned}$$

What emerges is:

(1) The equation $x \circ f = \mathbf{\Delta}_A$ does not necessarily have unique $x$-solutions, not even when only total solutions are sought.
(2) The equation $x \circ f = \mathbf{\Delta}_A$ *can* have *nontotal* $x$-solutions. Neither a total nor a nontotal solution is necessarily 1-1.
(3) An $x$-solution to $x \circ f = \mathbf{\Delta}_A$ can be 1-1 without being total.
(4) The equation $g \circ x = \mathbf{\Delta}_A$ does not necessarily have unique $x$-solutions. Solutions do not have to be onto. □

In the previous example we saw what we *cannot* infer about $f$ and $g$ from $g \circ f = \mathbf{\Delta}_A$. Let us next see what we *can* infer.

**V.3.4 Proposition.** *Given $f : \mathbb{A} \to \mathbb{B}$ and $g : \mathbb{B} \to \mathbb{A}$ such that $g \circ f = \mathbf{\Delta}_{\mathbb{A}}$. Then*

(1) *$f$ is total and* 1-1.
(2) *$g$ is onto.*

*Proof.* (1): Since $g \circ f$ is total, it follows that $f$ is too (for $f(a) \uparrow$ implies $g(f(a)) \uparrow$). Next, let $f(a) = f(b)$. Then $g(f(a)) = g(f(b))$ by Leibniz axiom; hence $g \circ f(a) = g \circ f(b)$, that is, $\mathbf{\Delta}_{\mathbb{A}}(a) = \mathbf{\Delta}_{\mathbb{A}}(b)$.

Hence $a = b$.

(2): For ontoness of $g$ we argue that there exists an $x$-solution of the equation $g(x) = a$ for any $a \in \mathbb{A}$. Indeed, $x = f(a)$ is a solution. □

**V.3.5 Corollary.** *Not all functions $f : \mathbb{A} \to \mathbb{B}$ have left (or right) inverses.*

*Proof.* Not all functions $f : \mathbb{A} \to \mathbb{B}$ are 1-1 (respectively, onto). □

**V.3.6 Corollary.** *Functions with neither left nor right inverses exist.*

*Proof.* Any $f : \mathbb{A} \to \mathbb{B}$ which is neither 1-1 nor onto fills the bill. For example, take $f = \{\langle 1, 2\rangle, \langle 2, 2\rangle\}$ from $\{1, 2\}$ to $\{1, 2\}$. □

☡ The above proofs can be thought of as *argot* versions of formal proofs, since 1 and 2 can be thought of as members of (the formal) $\omega$. ☡

**V.3.7 Proposition.** *If $f : \mathbb{A} \to \mathbb{B}$ is a 1-1 correspondence* (cf. III.11.24)*, then $x \circ f = \mathbf{\Delta}_{\mathbb{A}}$ and $f \circ x = \mathbf{\Delta}_{\mathbb{B}}$ have the* unique *common solution $f^{-1}$.*

N.B. This unique common solution, $f^{-1}$, is called *the inverse* of $f$.

*Proof.* First off, it is trivial that $f^{-1}$ is single-valued and hence a function. Verify next that it is a common solution:

$$\begin{aligned} af \circ f^{-1}b \quad &\text{iff} \quad (\exists c)(afc \wedge cf^{-1}b)\\ &\text{iff} \quad (\exists c)(afc \wedge bfc)\\ &\text{iff} \quad a = b \qquad (f \text{ is single-valued}) \end{aligned}$$

where the if part of the last iff is due to ontoness of $f$, while the only-if part employs proof by auxiliary constant (let $c$ work, i.e., $afc \wedge bfc \ldots$). Thus $x = f^{-1}$ solves $f \circ x = \mathbf{\Delta}_{\mathbb{B}}$. Similarly, one can show that it solves $x \circ f = \mathbf{\Delta}_{\mathbb{A}}$ too.

Uniqueness of solution: Let $x \circ f = \mathbf{\Delta}_{\mathbb{A}}$. Then $(x \circ f) \circ f^{-1} = \mathbf{\Delta}_{\mathbb{A}} \circ f^{-1} = f^{-1}$. By associativity of $\circ$, this says $x \circ (f \circ f^{-1}) = f^{-1}$, i.e., $x = x \circ \mathbf{\Delta}_{\mathbb{B}} = f^{-1}$. Therefore a left inverse has to be $f^{-1}$. The same can be similarly shown for the right inverse. □

**V.3.8 Corollary.** *If $f : \mathbb{A} \to \mathbb{B}$ has both left and right inverses, then it is a 1-1 correspondence, and hence the two inverses equal $f^{-1}$.*

*Proof.* From $h \circ f = \boldsymbol{\Delta}_{\mathbb{A}}$ ($h$ is some left inverse) it follows that $f$ is 1-1 and total. From $f \circ g = \boldsymbol{\Delta}_{\mathbb{B}}$ ($g$ is some right inverse) it follows that $f$ is onto. □

**V.3.9 Theorem (Algebraic Characterization of 1-1ness and Ontoness).**

(1) *$f : A \to B$ is total and* 1-1 *iff it is left-invertible.*[†]<br>
(2) *$g : B \to A$ is onto iff it is right-invertible.*[‡]

*Proof.* (1): The if part is Proposition V.3.4(1). As for the only-if part, note that $f^{-1} : B \to A$ is single-valued ($f$ is 1-1) and verify that $f^{-1} \circ f = \boldsymbol{\Delta}_A$.

(2): The *if part* is Proposition V.3.4(2).

*Only-if part:* By ontoness of $g$, all the *sets* in the family $\big(g^{-1}\langle x\rangle\big)_{x\in A}$ are nonempty. By AC, let $h \in \prod_{x\in A} g^{-1}\langle x\rangle$.

Thus, $h : A \to B$ is total, and $h(x) \in g^{-1}\langle x\rangle$ for *all* $x \in A$. Now, for all $x$,

$$\begin{aligned} h(x) \in g^{-1}\langle x\rangle \quad &\text{iff} \quad h(x)g^{-1}x \\ &\text{iff} \quad xg\,h(x) \\ &\text{iff} \quad x = g \circ h(x) \end{aligned}$$

That is, $g \circ h = \boldsymbol{\Delta}_A$. □

**V.3.10 Remark.** If $B \subseteq \mathbb{N}$, then AC is unnecessary in the proof of Theorem V.3.9 (case (2), only-if part).

Note that Theorem V.3.9 provides an "equational" or "algebraic" definition of ontoness and 1-1-ness (the latter for total functions). □

The reader has probably observed that, given $f : \mathbb{A} \to \mathbb{B}$ and $f^{-1} : \mathbb{B} \to \mathbb{A}$, an easy way to figure out the correct subscript of $\boldsymbol{\Delta}$ in $f \circ f^{-1} = \boldsymbol{\Delta}$ and $f^{-1} \circ f = \boldsymbol{\Delta}$ is to draw a diagram such as

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, "f^{-1}\circ f = 1_A"'] & B \arrow[d, "f^{-1}"] \\ & A \end{tikzcd}$$

[†] That is, it has a left inverse.

[‡] That is, it has a right inverse.

This is a trivial example of the usefulness of *function diagrams*. In some branches of mathematics, such as *category theory* and *algebraic topology*, it is an entire science to know how to manipulate complex function diagrams.

**V.3.11 Informal Definition (Function Diagrams).** A *function diagram* consists of a finite set of *points*, each labeled by some class (repetition of labels is allowed), and a finite set of *arrows* between points, each labeled by some function (*no* repetitions allowed).

If an arrow labeled $f$ *starts* (i.e., has its tail) at the (point labeled by the) class $\mathbb{X}$ and *ends* (i.e., has its head) at the class $\mathbb{Y}$, then the interpretation is that we have a function $f : \mathbb{X} \to \mathbb{Y}$.

A *chain* from point (labeled) $\mathbb{A}$ to point $\mathbb{B}$ in a diagram is a sequence of arrows in the diagram such that the first starts at $\mathbb{A}$, the last ends at $\mathbb{B}$, and the $(i + 1)$st starts where the $i$th ends, for all relevant $i$-values.

If $f_1, f_2, \ldots, f_n$ are the labels of a chain in that order from beginning to end, then we say that the chain has *length n* and *result* $f_n \circ f_{n-1} \circ \cdots \circ f_2 \circ f_1$.

A diagram is called *commutative* iff any two chains with common start and common end, of which *at least one* has length $\geq 2$, have the same result. □

**V.3.12 Example (Informal: *Examples of Function Diagrams*).**

(1) The following is commutative iff $g \circ f = h \circ f$. Note that commutativity does *not* require $g = h$, since both chains from $\mathbb{B}$ to $\mathbb{C}$ are of length one and thus the commutativity concept does not apply:

$$\begin{tikzcd} \mathbb{A} \arrow[r, "f"] & \mathbb{B} \arrow[r, shift left, "g"] \arrow[r, shift right, "h"'] & \mathbb{C} \end{tikzcd}$$

(2) The following is commutative:

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, "1_A"'] & B \arrow[d, "f^{-1}"] \\ & A \end{tikzcd}$$

(3) Recall that $\pi, \delta$ denote the first and second projections $\pi(\langle x, y\rangle) = x$ and $\delta(\langle x, y\rangle) = y$ for all $x, y$. Let $f : \mathbb{C} \to \mathbb{A}$ and $g : \mathbb{C} \to \mathbb{B}$ be two total functions. Then there is a *unique* total function $h$ which can label the dotted

arrow below and make the diagram commutative:

$$\begin{tikzcd}
 & A \\
C \arrow[ur, "f"] \arrow[r, dashed, "h"] \arrow[dr, "g"'] & A \times B \arrow[u, "\pi"'] \arrow[d, "\delta"] \\
 & B
\end{tikzcd}$$

This $h$ is, of course, $\lambda x.\langle f(x), g(x)\rangle : \mathbb{C} \to \mathbb{A} \times \mathbb{B}$.

Note that in drawing diagrams we do not draw the points; we only draw their labels. □

## V.4. Equivalence Relations

**V.4.1 Informal Definition.** A relation $\mathbb{P} : \mathbb{A} \to \mathbb{A}$ is an *equivalence relation on* $\mathbb{A}$ iff it is reflexive, symmetric, and transitive. □

Thus, in the metatheory "$\mathbb{P} : \mathbb{A} \to \mathbb{A}$ is an equivalence relation" means that "$\mathbb{P} \subseteq \mathbb{A} \times \mathbb{A}$ and $\mathbb{P}$ is reflexive, symmetric, and transitive" is *true*, whereas in ZFC it means that the quoted (quasi) translation[†] is *provable* (or has been taken as an assumption)

**V.4.2 Example.** As examples of equivalence relations we mention "=", i.e., $\mathbf{\Delta}$ on any class, and $\equiv$ (mod $m$) on $\mathbb{Z}$ (see Example V.2.17). □

An equivalence relation on $\mathbb{A}$ has the effect, intuitively, of grouping equivalent (i.e., related) elements into equivalence classes.

[†] The reflexive, symmetric, and transitive properties have trivial translations in the formal language.

Why is this intuition *not* valid for arbitrary relations? Well, for one thing, not all relations are symmetric, so if element $a$ of $\mathbb{A}$ started up a club of "pals" with respect to a (non-symmetric) relation $\mathbb{P}$, then $a$ would welcome $b$ into the club as soon as $a \,\mathbb{P}\, b$ holds. Now since, conceivably, $b \,\mathbb{P}\, a$ is false, $b$ would *not* welcome $a$ in *his* club. The two clubs would be different. Now that is contrary to the *intuitive* meaning of "equivalence" according to which we would like $a$ and $b$ to be in the same club.

O.K., so let us throw in symmetry. Do symmetric relations group related elements in a way we could intuitively call "equivalence"? Take the symmetric relation $\neq$. If it behaved like equivalence, then $a \neq b$ and $b \neq c$ would require all three $a, b, c$ to belong to the same "pals' club", for $a$ and $b$ are in the same club, *and* $b$ and $c$ are in the same club. Alas, it is conceivable that $a \neq b \neq c$, yet $a = c$, so that $a$ and $c$ would *not* be in the same club. The problem is that $\neq$ is not transitive.

What do we need reflexivity for? Well, without it we would have "stray" elements (of $\mathbb{A}$) which belong to no clubs at all, and this is undesirable intuitively. For example, $R = \{\langle 1,2\rangle, \langle 2,1\rangle, \langle 1,1\rangle, \langle 2,2\rangle\}$ is symmetric and transitive on $A = \{1,2,3\}$. We have exactly one club, $\{1,2\}$, and 3 belongs to no club. We fix this by adding $\langle 3,3\rangle$ to $R$, so that 3 belongs to the club $\{3\}$.

As we already said, intuitively we view related elements of an equivalence relation as indistinguishable. We collect them in so-called equivalence classes (the "clubs") which are therefore viewed *intuitively* as a kind of "fat urelements" (their individual members lose their "individuality").

Here are the technicalities.

**V.4.3 Informal Definition.** Given an equivalence relation $\mathbb{P}$ on $\mathbb{A}$. The *equivalence class* of an element $a \in \mathbb{A}$ is $\{x \in \mathbb{A} : x \,\mathbb{P}\, a\}$. We use the symbol $[a]_{\mathbb{P}}$, or just $[a]$ if $\mathbb{P}$ is understood, for the equivalence class.

If $\mathbb{P}$, $\mathbb{A}$ are *sets* $P$, $A$, then $A/P$, the *quotient set* of $A$ with respect to $P$, is the set of all equivalence classes $[a]_P$. □

(1) Restricting the definition of $A/P$ to sets $P$, $A$ ensures that $[x]_P$ are sets (why?) so that $A/P$ makes sense as a class. Indeed, it is a set, by collection.
(2) Of course, $[a]_{\mathbb{P}} = \mathbb{P}[\{a\}] = \mathbb{P}\langle a\rangle$.

**V.4.4 Lemma.** *Let* $\mathbb{P}$ *be an equivalence relation on* $\mathbb{A}$. *Then* $[x] = [y]$ *iff* $x \,\mathbb{P}\, y$.

*Proof. If part.* Let $z \in [x]$. Then $z \,\mathbb{P}\, x$. Hence $z \,\mathbb{P}\, y$ by assumption and transitivity. That is, $z \in [y]$, from which $[x] \subseteq [y]$.

By swapping letters we have $y \mathbb{P} x$ implies $[y] \subseteq [x]$; hence (by symmetry of $\mathbb{P}$) our original assumption, namely $x \mathbb{P} y$, implies $[y] \subseteq [x]$. All in all, $[x] = [y]$.

*Only-if part.* By reflexivity, $x \in [x]$. The assumption then yields $x \in [y]$, i.e., $x \mathbb{P} y$. □

**V.4.5 Lemma.** *Let $\mathbb{P}$ be an equivalence relation on $\mathbb{A}$. Then*

$(i)$ $[x] \neq \emptyset$ *for all* $x \in \mathbb{A}$.
$(ii)$ $[x] \cap [y] \neq \emptyset$ *implies* $[x] = [y]$ *for all* $x, y$ *in* $\mathbb{A}$.
$(iii)$ $\bigcup_{x \in \mathbb{A}} [x] = \mathbb{A}$.

*Proof.* $(i)$: From $x \mathbb{P} x$ for all $x \in \mathbb{A}$ we get $x \in [x]$.

$(ii)$: Let $z \in [x] \cap [y]$. Then $z \mathbb{P} x$ and $z \mathbb{P} y$; therefore $x \mathbb{P} z$ and $z \mathbb{P} y$ (by symmetry); hence $x \mathbb{P} y$ (by transitivity). Thus, $[x] = [y]$ by Lemma V.4.4.

$(iii)$: The $\subseteq$-part is obvious from $[x] \subseteq \mathbb{A}$. The $\supseteq$-part follows from $\bigcup_{x \in \mathbb{A}} \{x\} = \mathbb{A}$ and $\{x\} \subseteq [x]$. □

The properties $(i)$–$(iii)$ are characteristic of the notion of a *partition of a set*.

**V.4.6 Definition (Partitions).** Let $(F_a)_{a \in I}$ be a family of subsets of $A$. It is a *partition of $A$* iff all of the following hold:

$(i)$ $F_a \neq \emptyset$ for all $a \in I$.
$(ii)$ $F_a \cap F_b \neq \emptyset$ implies $F_a = F_b$ for all $a, b$ in $I$.
$(iii)$ $\bigcup_{x \in I} F_a = A$. □

There is a natural affinity between equivalence relations and partitions on a set $A$.

**V.4.7 Theorem.** *The relation $C = \{\langle R, A/R \rangle : R$ is an equivalence relation on $A\}$ is a 1-1 correspondence between the set $\mathscr{E}$ of all equivalence relations on $A$ and the set $\mathscr{P}$ of all partitions on $A$.*

**Pause.** Are all the "sets" mentioned in the theorem indeed sets?

*Proof.* By definition, $C$ is single-valued (on the $\delta$-coordinate) on $\mathscr{E}$ and total, since whenever $R$ occurs in $\langle R, x \rangle$, $x$ is always the same, namely, $A/R$. Moreover, for each $R \in \mathscr{E}$, $A/R$ exists. By Lemma V.4.5 $\mathrm{ran}(C) \subseteq \mathscr{P}$, so that we have a *total* function $C : \mathscr{E} \to \mathscr{P}$ so far.

We next check ontoness:

Let $\Pi = (F_a)_{a \in I} \in \mathscr{P}$. Define a relation $\widehat{\Pi}$ on $A$ as follows:

$$x \,\widehat{\Pi}\, y \quad \text{iff} \quad (\exists a \in I)\{x, y\} \subseteq F_a$$

Observe that:

(i) $\widehat{\Pi}$ is reflexive: Take any $x \in A$. By V.4.6(iii), there is an $a \in I$ such that $x \in F_a$, and hence $\{x, x\} \subseteq F_a$. Thus $x \,\widehat{\Pi}\, x$.

(ii) $\widehat{\Pi}$ is, trivially, symmetric.

(iii) $\widehat{\Pi}$ is transitive: Indeed, let $x \,\widehat{\Pi}\, y \,\widehat{\Pi}\, z$. Then $\{x, y\} \subseteq F_a$ and $\{y, z\} \subseteq F_b$ for some $a, b$ in $I$. Thus, $y \in F_a \cap F_b$; hence $F_a = F_b$ by V.4.6(ii). Hence $\{x, z\} \subseteq F_a$; therefore $x \,\widehat{\Pi}\, z$.

So $\widehat{\Pi}$ is an equivalence relation. Once we show that $C(\widehat{\Pi}) = \Pi$, i.e., $A/\widehat{\Pi} = \Pi$, we will have settled ontoness.

$\subseteq$: Let $[x]$ be arbitrary in $A/\widehat{\Pi}$ (we use $[x]$ for $[x]_{\widehat{\Pi}}$). Take $F_a$ such that $x \in F_a$ (it exists by V.4.6(iii)). Now let $z \in [x]$. Then $z \,\widehat{\Pi}\, x$; hence $z, x$ are in the same $F_b$, which is $F_a$ by V.4.6(ii). Hence $z \in F_a$; therefore $[x] \subseteq F_a$.

Conversely, if $z \in F_a$, since also $x \in F_a$, then $z \,\widehat{\Pi}\, x$; thus $z \in [x]$. All in all, $[x] = F_a$, where $F_a$ is *the unique* $F_a$ containing $x$. Thus $[x] \in \Pi$.

$\supseteq$: Let $F_a$ be arbitrary in $\Pi$. By V.4.6(i), there is some $x \in F_a$. By the same argument as in the $\subseteq$-part, $[x] = F_a$; thus $F_a \in A/\widehat{\Pi}$.

For 1-1-ness, let $\Pi$ and $\widehat{\Pi}$ be as before, and let also $R \in \mathscr{E}$ such that $A/R = \Pi$. If $x \, R \, y$, then $[x]_R = [y]_R$. Let $[x]_R = F_a$ for some $a \in I$; thus $x$ and $y$ are in $F_a$, that is, $x \,\widehat{\Pi}\, y$. The argument is clearly reversible, so $R = \widehat{\Pi}$. □

**V.4.8 Example (Informal).** The equivalence relation $\equiv_m$ on $\mathbb{Z}$ determines the quotient set $\mathbb{Z}/\equiv_m = \big\{\{i + k \cdot m : k \in \mathbb{Z}\} : i \in \mathbb{Z} \wedge 0 \leq i < m\big\}$. We usually denote $\mathbb{Z}/\equiv_m$ by $\mathbb{Z}_m$. □

**V.4.9 Example.** Given $f : A \to B$. Define $R_f$ by

$$x \, R_f \, y \quad \text{iff} \quad f(x) \simeq f(y) \tag{1}$$

where $\simeq$ is the weak equality of Kleene (see III.11.17).

$R_f$ is an equivalence relation:

(i) For all $x \in A$ we have $f(x) \simeq f(x)$; hence $x \, R_f \, x$ (this would have failed whenever $f(x) \uparrow$ if we had used $=$ rather than $\simeq$ in (1)).

(ii) $R_f$ is trivially symmetric.

(iii) $R_f$ is transitive: $x \; R_f \; y \; R_f \; z$ means $f(x) \simeq f(y) \simeq f(z)$, and hence $f(x) \simeq f(z)$, and hence $x \; R_f \; z$.

We can, intuitively, "lump" or "identify" all "points" in $A$ that map into the same element of $B$, thus, in essence, turning $f$ into a 1-1 function. We also lump together all points of $A$ for which $f$ is undefined. All this is captured by the following commutative diagram:

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "h = \lambda x.[x]"'] & B \\
A/R_f \arrow[ur, "g = \lambda [x].f(x)"'] &
\end{tikzcd}$$

We observe:

(a) $\lambda x.[x]$ is total and onto. It is called the *natural projection of A onto* $A/R_f$.[†]
(b) $[x] \mapsto f(x)$ is single-valued,[‡] for if $[x] = [y]$, then $x \; R_f \; y$ and thus $f(x) \uparrow \wedge f(y) \uparrow \vee (\exists z)(z = f(x) \wedge z = f(y))$.
(c) The function $[x] \mapsto f(x)$ is defined iff $f(x) \downarrow$ (trivial).
(d) $[x] \mapsto f(x)$ is 1-1. For, let $\langle [x], a \rangle$ and $\langle [y], a \rangle$ be pairs of this function. The first pair implies $f(x) = a$, and the second implies $f(y) = a$, thus $f(x) = f(y)$, and hence $f(x) \simeq f(y)$. It follows that $x \; R_f \; y$, and hence $[x] = [y]$.
(e) Let $h = \lambda x.[x]$ and $g = \lambda [x].f(x)$. Then $g \circ h(x) = g(h(x)) = g([x]) = f(x)$.
This verifies the earlier claim that the above diagram is commutative.

[†] The term applies to the general case $\lambda x.[x] : A \to A/R$, not just for the special $R = R_f$ above.

[‡] In this context one often says "well-defined", i.e., the image $f(x)$ is independent of the *representative x* which denotes (defines) the equivalence class $[x]$.

(f) The moral, in words, is: "Every function $f : A \to B$ can be decomposed into a *1-1* and an *onto total* function, in that left-to-right order. Moreover, the 1-1 component is total iff $f$ is." □

## V.5. Exercises

**V.1.** *Course-of-values induction.* Prove that for any formula $\mathscr{F}(x)$,

$$\text{ZFC} \vdash (\forall n \in \omega)\big((\forall m < n \in \omega)\mathscr{F}(m) \to \mathscr{F}(n)\big) \to (\forall n \in \omega)\mathscr{F}(n)$$

or, in words, if for the arbitrary $n \in \omega$ we can prove $\mathscr{F}(n)$ on the *induction hypothesis* that $\mathscr{F}(m)$ holds for *all* $m < n$, then this is as good as having proved $(\forall n \in \omega)\mathscr{F}(n)$.

(*Hint.* Assume $(\forall n \in \omega)\big((\forall m < n \in \omega)\mathscr{F}(m) \to \mathscr{F}(n)\big)$ to prove $(\forall n \in \omega)\mathscr{F}(n)$. Consider the formula $\mathscr{G}(n)$ defined as $(\forall m < n \in \omega)\mathscr{F}(m)$, and apply (ordinary) induction on $n$ to prove that $(\forall n \in \omega)\mathscr{G}(n)$. Take it from there.)

**V.2.** *The "least" number principle over $\omega$.* Prove that every $\emptyset \neq A \subseteq \omega$ has a *minimal* element, i.e., an $n \in A$ such that for no $m \in A$ is it possible to have $m < n$. Do so without foundation, using instead course-of-values induction.

**V.3.** Prove that the principle of induction over $\omega$ and the least number principle are equivalent, i.e., one implies the other. Again, do so without using foundation.

**V.4.** Redo the proof of Theorem V.1.21 (existence part) so that it would go through even if trichotomy of $\in$ over $\omega$ did not hold.

**V.5.** Prove that a set $x$ is a natural number iff it satisfies (1) and (2) below:
(1) It and all its members are transitive.
(2) It and all its members are successors or $\emptyset$.

**V.6.** Prove that for all $m, n, i$ in $\omega$, $m + (n + i) = (m + n) + i$.

**V.7.** Redo the proof of V.1.24 (commutativity of natural number addition) by a *single* induction, relying on the associativity of addition.

**V.8.** Prove that for all $m$ in $\omega$, $m < n$ implies $m + 1 \leq n$ (recall that $\leq$ on $\omega$ is the same as $\subseteq$).

**V.9.** Prove that for all $m, n$ in $\omega$, $m < n$ implies $m + 1 < n + 1$.

**V.10.** Show by an appropriate example that if $f$, $g$ are finite sequences, then $f * g \neq g * f$ in general.

**V.11.** Define *multiplication*, "$\cdot$", on $\omega$ by

$$\begin{aligned} m \cdot 0 &= 0 \\ m \cdot (n+1) &= m \cdot n + m \end{aligned}$$

Prove:

(1) $\cdot$ is associative.

(2) $\cdot$ is commutative.

(3) $\cdot$ distributes over $+$, i.e., for all $m, n, k$, $(m+n)\cdot k = (m \cdot k) + (n \cdot k)$.

**V.12.** Prove that $m + n < (m+1)\cdot(n+1)$ for all $m, n$ in $\omega$.

**V.13.** Let $\mathbb{P}$ be both symmetric and antisymmetric. Show that $\mathbb{P} \subseteq \mathbf{\Delta}_{\mathbb{A}}$, where $\mathbb{A}$ is the field of $\mathbb{P}$. Conclude that $\mathbb{P}$ is transitive.

**V.14.** In view of the previous problem, explore the patterns of independence between reflexivity, symmetry, antisymmetry, transitivity, and irreflexivity.

**V.15.** For any relation $\mathbb{P}$, $(\mathbb{P}^{-1})^{-1} = \mathbb{P}$.

**V.16.** Let $R : A \to A$ be a relation (set). Define

$$\begin{aligned} P &= \{S \subseteq A \times A : R \subseteq S \wedge S \text{ is reflexive}\} \\ Q &= \{S \subseteq A \times A : R \subseteq S \wedge S \text{ is symmetric}\} \\ T &= \{S \subseteq A \times A : R \subseteq S \wedge S \text{ is transitive}\} \end{aligned}$$

Show that

$$\begin{aligned} r(R) &= \bigcap P \\ s(R) &= \bigcap Q \\ t(R) &= \bigcap T \end{aligned}$$

**V.17.** Fill in the missing details of Example V.2.29.

**V.18.** If $R$ is on $A = \{1, \ldots, n\}$, then show that

$$R^+ = \bigcup_{i=1}^{n} R^i$$

**V.19.** If $R$ is reflexive on $A = \{1, \ldots, n\}$, then

$$R^+ = R^{n-1}$$

**V.20.** Show that for any $\mathbb{P} : \mathbb{A} \to \mathbb{A}$, $s(r(\mathbb{P})) = r(s(\mathbb{P}))$.

**V.21.** Show by an appropriate example that, in general, $s(t(\mathbb{P})) \neq t(s(\mathbb{P}))$.

**V.22.** Given $R$ on $A = \{1, \ldots, n\}$.

(a) Prove by an appropriate induction that the following algorithm terminates with the value $A_{R^+}$ in the matrix variable $M$:

```
$M \leftarrow A_R$
**for** $i = 1$ **to** $n - 1$ **do**
    $M \leftarrow (A_\Delta + M) \cdot A_R$
```

(b) Show that the above algorithm performs $O(n^4)$ operations of the type "+" and "·".

$f(n) = O(g(n))$ means $|f(n)| \le C \cdot |g(n)|$ for all $n \ge n_0$ (for some constants $C, n_0$ independent of $n$), or, equivalently, $|f(n)| \le C \cdot |g(n)| + D$ for all $n \ge 0$ (for some constants $C$, $D$ independent of $n$).

**V.23.** (a) Prove that if $R$ is on $A = \{1, \ldots, n\}$, then $R^+ = \bigcup_{i=1}^{m} R^i$ for all $m \ge n$.

(b) Based on the above observation, on Example V.2.35, and on the fact (with proof, of course) that for any matrix $M$ we can find $M^{2^k}$ in $k$ matrix multiplications, find an algorithm that *provably* computes $R^+$ in $O(n^3 \log n)$ operations of the type "+" and "·".

**V.24.** Prove by appropriate inductions that the following algorithm due to Warshall terminates with the value $A_{R^+}$ in the matrix variable $M$, and that all this is done in $O(n^3)$ "+"-operations (there are no "·"-operations in this algorithm):

```
$M \leftarrow A_R$
**for** $j = 1$ **to** $n$ **do**
    **for** $i = 1$ **to** $n$ **do**
     **if** $M(i, j) = 1$ **then**
          **for** $k = 1$ **to** $n$ **do**
             $M(i, k) \leftarrow M(i, k) + M(j, k)$
     **fi**
```

Is the algorithm still correct if the first two loops are interchanged (i.e., if $i$ is controlled by the outermost loop, rather than $j$)?

(*Hint*. When $M(i, j) = 1$, $M(i, k) \leftarrow M(i, k) + M(j, k)$ says the same thing as $M(i, k) \leftarrow M(i, k) + M(i, j) \cdot M(j, k)$.)

**V.25.** Prove that for sets $P$, $A$, where $P$ is an equivalence relation on $A$, $A/P$ is a set as Definition V.4.3 wants us believe.

# VI

# Order

This chapter contains concepts that are fundamental for the further development of set theory, such as *well-orderings* and *ordinals*. The latter constitute the skeleton of set theory, as they formalize the intuitive concept of "stages" and, among other things, enable us to make transfinite constructions *formally* (such as the construction of the universe of sets and atoms, $\mathbb{U}_M$, and the constructible universe, $\mathbb{L}_M$).

## VI.1. PO Classes, LO Classes, and WO Classes

We start with the introduction of the most important type of binary relation, that of *partial order*.

**VI.1.1 Definition.** A relation $\mathbb{P}$ is a *partial order*, or just *order*, iff it is

(1) *irreflexive* (i.e., $x \,\mathbb{P}\, y \to \neg x = y$) and
(2) *transitive*.

It is emphasized that $\mathbb{P}$ need not be a set. □

**VI.1.2 Remark.**

(1) The symbol $<$ will be used to denote *any* unspecified order $\mathbb{P}$, and it will be pronounced "less than". It is hoped that the context will not allow confusion with the concrete $<$ on numbers (say, on the reals).
(2) If the field of the order $<$ is a subclass of $\mathbb{A}$, then we say that $<$ *is an order on* $\mathbb{A}$.
(3) Clearly, for any order $<$ and any class $\mathbb{B}$, $< \cap (\mathbb{B} \times \mathbb{B})$ – or $< \mid \mathbb{B}$ – is an order on $\mathbb{B}$. □

**VI.1.3 Example (Informal).** The concrete "less than", $<$, on $\mathbb{N}$ is an order, but $\leq$ is not (it is not irreflexive). The "greater than" relation, $>$, on $\mathbb{N}$ is also an order, but $\geq$ is not.

In general, it is trivial to verify that $\mathbb{P}$ is an order iff $\mathbb{P}^{-1}$ is an order. □

**VI.1.4 Example.** $\emptyset$ is an order. Since for any $\mathbb{A}$ we have $\emptyset \subseteq \mathbb{A} \times \mathbb{A}$, $\emptyset$ is an order *on* $\mathbb{A}$ for the arbitrary $\mathbb{A}$. □

**VI.1.5 Example.** The relation $\in$ (strictly speaking, the relation defined by the *formula* $x \in y$ – see III.11.2) is irreflexive by the foundation axiom. It is not transitive, though. For example, if $a$ is a set (or atom), then $a \in \{a\} \in \{\{a\}\}$ but $a \notin \{\{a\}\}$.

Let $A = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}$. The relation $\varepsilon = \in \cap (A \times A)$ is transitive and irreflexive; hence it is an order (on $A$). □

**VI.1.6 Example.** $\subset$ is an order; $\subseteq$ – failing irreflexivity – is not. □

**VI.1.7 Definition.** Let $<$ be a partial order on $\mathbb{A}$. We use the abbreviation $\leq$ for $r_{\mathbb{A}}(<) = \Delta_{\mathbb{A}} \cup <$. We pronounce $\leq$ "less than or equal". $r_{\mathbb{A}}(>)$, i.e., $r_{\mathbb{A}}(<^{-1})$ is denoted by $\geq$ and is pronounced "greater than or equal". □

(1) In plain English, given $<$ on $\mathbb{A}$, we define $x \leq y$ to mean $x < y \vee x = y$ for all $x, y$ in $\mathbb{A}$.
(2) The definition of $\leq$ depends on $\mathbb{A}$, due to the presence of $\Delta_{\mathbb{A}}$. There is no such dependence on a "reference" or "carrier" class in the case of $<$.

**VI.1.8 Lemma.** *For any* $<\colon \mathbb{A} \to \mathbb{A}$, *the associated* $\leq$ *on* $\mathbb{A}$ *is reflexive, antisymmetric, and transitive.*

*Proof.* (1) Reflexivity is trivial.

(2) For antisymmetry, let $x \leq y$ and $y \leq x$. If $x = y$ then we are done, so assume the remaining case $x \neq y$ (i.e., $\langle x, y\rangle \notin \Delta_{\mathbb{A}}$). Then the hypothesis becomes $x < y$ and $y < x$; therefore $x < x$ by transitivity, contradicting the irreflexivity of $<$.

(3) As for transitivity, let $x \leq y$ and $y \leq z$. If $x = z$, then $x \leq z$ (see the remark following VI.1.7) and we are done. The remaining case is $x \neq z$. Now, if $x = y$ or $y = z$, then we are done again; so it remains to consider the case $x < y$ and $y < z$. By transitivity of $<$ we get $x < z$, and hence $x \leq z$, since $< \subseteq \leq$. □

**VI.1.9 Lemma.** *Let $\mathbb{P}$ on $\mathbb{A}$ be reflexive, antisymmetric, and transitive. Then $\mathbb{P} - \Delta_{\mathbb{A}}$ is an order on $\mathbb{A}$.*

*Proof.* Since

$$\mathbb{P} - \Delta_{\mathbb{A}} \subseteq \mathbb{P} \tag{1}$$

it is clear that $\mathbb{P} - \Delta_{\mathbb{A}}$ is *on* $\mathbb{A}$. It is also clear that it is irreflexive. We only need verify that it is transitive.

So let

$$\langle x, y\rangle \text{ and } \langle y, z\rangle \text{ be in } \mathbb{P} - \Delta_{\mathbb{A}} \tag{2}$$

By (1)

$$\langle x, y\rangle \text{ and } \langle y, z\rangle \text{ are in } \mathbb{P} \tag{3}$$

Hence

$$\langle x, z\rangle \in \mathbb{P}$$

by transitivity of $\mathbb{P}$.

Can $\langle x, z\rangle \in \Delta_{\mathbb{A}}$, i.e., can $x = z$? No, for antisymmetry of $\mathbb{P}$ and (3) would imply $x = y$, i.e., $\langle x, y\rangle \in \Delta_{\mathbb{A}}$, contrary to (2).

So $\langle x, z\rangle \in \mathbb{P} - \Delta_{\mathbb{A}}$. □

**VI.1.10 Remark.** Often in the literature $\leq : \mathbb{A} \to \mathbb{A}$ is defined as a partial order by the requirements that it be reflexive, antisymmetric, and transitive. Then $<$ is obtained as in Lemma VI.1.9, namely, as $\leq - \Delta_{\mathbb{A}}$. Lemmata VI.1.8 and VI.1.9 show that the two approaches are interchangeable, but the modern approach of Definition VI.1.1 avoids the nuisance of tying the notion of order to some particular carrier class $\mathbb{A}$. For us "$\leq$" is the *derived* notion from VI.1.7. □

**VI.1.11 Informal Definition.** If $<$ is an order on a class $\mathbb{A}$, we call the pair[†] $(\mathbb{A}, <)$ a *partially ordered class*, or *PO class*. If $<$ is an order on a *set* $A$, then we call the pair $(A, <)$ a *partially ordered set* or *PO set*. Often, if the order $<$ is understood as being on $\mathbb{A}$ or $A$, one says that "$\mathbb{A}$ is a PO class" or "$A$ is a PO set" respectively. □

**VI.1.12 Example (Informal).** Consider the order $\subset$ once more. In this case we have none of $\{\emptyset\} \subset \{\{\emptyset\}\}$, $\{\{\emptyset\}\} \subset \{\emptyset\}$ or $\{\{\emptyset\}\} = \{\emptyset\}$. That is, $\{\emptyset\}$ and $\{\{\emptyset\}\}$

[†] Formally, $(\mathbb{A}, <)$ is *not* an ordered pair $\langle \ldots \rangle$, for $\mathbb{A}$ may be a proper class. We may think then of "$(\mathbb{A}, <)$" as *informal* notation that simply "ties" $\mathbb{A}$ and $<$ together. If we were absolutely determined to, then we could introduce pairing with proper classes as components, for example as $(\mathbb{A}, \mathbb{B}) = (\mathbb{A} \times \{0\}) \cup (\mathbb{B} \times \{1\})$. For our part we will have no use for such pair types and will consider $(\mathbb{A}, <)$ in the informal sense.

are *non-comparable* items. This justifies the qualification *partial* for orders in general (Definition VI.1.1).

On the other hand, the "natural" $<$ on $\mathbb{N}$ is such that one of $x = y$, $x < y$, $y < x$ always holds for any $x, y$ (trichotomy). That is, all (unordered) pairs $x, y$ of $\mathbb{N}$ *are* comparable under $<$. This is a concrete example of a *total* order. Another example is $\in$ on $\omega$ (V.1.20).

While *all* orders are partial orders, some are total ($<$ above) and others are nontotal ($\subset$ above). □

**VI.1.13 Definition.** A relation $<$ on $\mathbb{A}$ is a *total* or *linear* order *on* $\mathbb{A}$ iff

(1) it is an order, and
(2) for any $x, y$ in $\mathbb{A}$ one of $x = y,\ x < y,\ y < x$ holds (*trichotomy*).

If $\mathbb{A}$ is a class, then the pair $(\mathbb{A}, <)$ is a *linearly ordered class*, or *LO class*. If $\mathbb{A}$ is a set, then the pair $(\mathbb{A}, <)$ is a *linearly ordered set*, or *LO set*. One often calls just $\mathbb{A}$ a LO class or LO set (as the case warrants) when $<$ is understood from the context. □

**VI.1.14 Example (Informal).** The standard $<: \mathbb{N} \to \mathbb{N}$ is a total order; hence $(\mathbb{N}, <)$ is a LO set. □

**VI.1.15 Definition.** Let $<$ be an order and $\mathbb{A}$ some class. An element $a \in \mathbb{A}$ is *a $<$-minimal element in* $\mathbb{A}$, or *a $<$-minimal element of* $\mathbb{A}$, iff $\neg(\exists x \in \mathbb{A})x < a$.

$m \in \mathbb{A}$ is *a $<$-minimum element in* $\mathbb{A}$ iff $(\forall x \in \mathbb{A})m \leq x$.

We also use the terminology minimal or minimum *with respect to* $<$, instead of $<$-minimal or $<$-minimum.

If $a \in \mathbb{A}$ is $>$-minimal in $\mathbb{A}$, that is, $\neg(\exists x \in \mathbb{A})x > a$, we call $a$ a *$<$-maximal element* in $\mathbb{A}$. Similarly, a $>$-minimum element is called a *$<$-maximum element*.

If the order $<$ is understood, then the qualification "$<$-" is omitted. □

In particular, if $a \in \mathbb{A}$ is *not* in the field of $<$, then $a$ is *both* $<$-minimal and $<$-maximal *in* $\mathbb{A}$.

Note that minimality with respect to $<$ in $\mathbb{A}$ has the interesting formulation $< \langle a \rangle \cap \mathbb{A} = \emptyset$, which, *if $<$ is on* $\mathbb{A}$, simplifies further to $< \langle a \rangle \uparrow$. In this light, the "general case" also reads $\big(< \mid \mathbb{A}\big)\langle a \rangle \uparrow$ (see III.11.9), i.e., $a \in \mathbb{A}$ is $<$-minimal iff the (relational) restriction of $<$ on $\mathbb{A}$ is undefined at $a$.

Because of the duality between the notions of minimal/maximal and minimum/maximum, we will mostly deal with the $<$-notions, whose results can be trivially translated for the $>$-notions.

**VI.1.16 Example (Informal).** 0 is *minimal*, and also *minimum*, in $\mathbb{N}$ with respect to the natural ordering.

In $\mathbf{P}(\mathbb{N})$, $\emptyset$ is both $\subset$-minimal and $\subset$-minimum. On the other hand, all of $\{0\}, \{1\}, \{2\}$ are $\subset$-minimal in $\mathbf{P}(\mathbb{N}) - \{\emptyset\}$ but *none* are $\subset$-*minimum* in that set.

Observe from this last example that minimal elements in a class are *not in general* unique. □

**VI.1.17 Lemma.** *Given an order $<$ and a class $\mathbb{A}$.*

(1) *If $m$ is a minimum in $\mathbb{A}$, then it is also minimal.*
(2) *If $m$ is a minimum in $\mathbb{A}$, then it is unique.*

*Proof.* (1): Assume

$$(\forall x \in \mathbb{A})(m = x \lor m < x) \tag{$i$}$$

and prove $\neg(\exists x \in \mathbb{A})x < m$.

Well, assume $(\exists x \in \mathbb{A})x < m$ instead, and introduce a new constant $a$ with the assumption $a < m \land a \in \mathbb{A}$. By $(i)$, $m = a \lor m < a$. Now, by irreflexivity, case $m = a$ is ruled out. But then case $m < a$ and transitivity yield $a < a$, which contradicts irreflexivity.

(2): Let $m$ and $n$ be minima[†] in $\mathbb{A}$. Then $m \le n$ (with $m$ posing as minimum) and $n \le m$ (now $n$ is so posing); hence $m = n$ by antisymmetry (Lemma VI.1.8). □

**VI.1.18 Example.** Let $m$ be $<$-minimal in $\mathbb{A}$. Let us attempt to show that it is also $<$-minimum (this is, of course, doomed to fail due to VI.1.16 and VI.1.17(2) – but the false proof below is interesting).

By VI.1.15 we have $\neg(\exists x \in \mathbb{A})x < m$. That is, $(\forall x \in \mathbb{A})\neg x < m$, i.e., $(\forall x \in \mathbb{A})m \le x$, which says that $m$ is $<$-minimum in $\mathbb{A}$.

The error is in the last step, where $\neg x < m$ and $m = x \lor m < x$ were taken to be equivalent – i.e., we unjustifiably assumed trichotomy or totalness of the order "$<$". As we have seen (VI.1.16), it *is* possible to prove all three of $\neg x < m, \neg x = m, \neg m < x$ for some orders and appropriate $x$ and $m$. □

**VI.1.19 Lemma.** *If $<$ is a* linear *order on $\mathbb{A}$, then every minimal element is also minimum.*

[†] Plural of minimum.

*Proof.* The false proof of the previous example is valid under the present circumstances. □

Much is to be gained, especially for work we will be doing in the next section, if we generalize the notion of "minimal" – and, dually, "maximal" – (Definition VI.1.15) to make it relevant to *any* relation $\mathbb{P}$, even one that is not necessarily an order.

**VI.1.20 Definition.** Let $\mathbb{P}$ be some relation and $\mathbb{A}$ some class.

We say that $a \in \mathbb{A}$ is $\mathbb{P}$*-minimal in* $\mathbb{A}$ – or a $\mathbb{P}$*-minimal element of* $\mathbb{A}$ – iff $\mathbb{P} \mid \mathbb{A}\langle a\rangle \uparrow$.[†]

If $a$ is $\mathbb{P}^{-1}$*-minimal in* $\mathbb{A}$, then we call it $\mathbb{P}$*-maximal in* $\mathbb{A}$. □

**VI.1.21 Remark.** Clearly, Definition VI.1.15 is a special case of VI.1.20 when $\mathbb{P}$ is an order. For $a \in \mathbb{A}$ the condition $\mathbb{P} \mid \mathbb{A}\langle a\rangle \uparrow$ is equivalent to $\mathbb{A} \cap \mathbb{P}\langle a\rangle = \emptyset$, since

$$\mathbb{P} \mid \mathbb{A}\langle a\rangle = \begin{cases} \emptyset & \text{if } a \notin \mathbb{A} \\ \mathbb{A} \cap \mathbb{P}\langle a\rangle & \text{otherwise} \end{cases}$$

□

The following type of relation has crucial importance for set theory, and mathematics in general.

**VI.1.22 Informal Definition.** A relation $\mathbb{P}$ (not necessarily an order) satisfies the *minimal condition* (briefly, *it has MC*) iff every nonempty $\mathbb{A}$ has $\mathbb{P}$-minimal elements.

If a *total* order $<: \mathbb{A} \to \mathbb{A}$ has MC, then it is a *well-ordering on* (or *of*) the class $\mathbb{A}$.

If $(\mathbb{A}, <)$ is a LO class (or set) with MC, then it is a *well-ordered*, or *WO, class* (or set). □

**VI.1.23 Remark (The Formalities – Exegesis).** The above informal definition is worded semantically (most informal definitions are), saying what an inhabitant of $\mathbb{U}_M$ ought to look for to recognize that a relation $\mathbb{P}$ has MC. Since *we* insist on certifying truths via proofs in ZFC (notwithstanding our knowledge that not all truths are so certifiable), *operationally*, we have so certified some

[†] As in the case where we wrote "<" for "$\mathbb{P}$" (VI.1.15), the symbol "|" is taken to have higher priority than "$\langle a\rangle$" and "$\uparrow$"; thus "$\mathbb{P} \mid \mathbb{A}\langle a\rangle \uparrow$" means "$\big(\mathbb{P} \mid \mathbb{A}\big)\langle a\rangle \uparrow$".

relation $\mathbb{P}$ – and proclaimed that "$\mathbb{P}$ has MC" – just in case we have proved the schema[†]

$$\emptyset \neq \mathbb{A} \to (\exists x \in \mathbb{A})\mathbb{A} \cap \mathbb{P}\langle x\rangle = \emptyset \tag{1}$$

Correspondingly, the phrase "let $\mathbb{P}$ have MC" is *argot* for the phrase "add the axiom schema (1)".

In the present connection, if we set $\mathbb{A} = \{x : \mathscr{A}[x]\}$, schema (1) translates into

$$(\exists x)\mathscr{A}[x] \to (\exists x)\big(\mathscr{A}[x] \wedge \neg(\exists y)(y\,\mathbb{P}\,x \wedge \mathscr{A}[y])\big) \tag{2}$$

and each specific formula $\mathscr{A}$ provides an instance (see also VI.1.25 below).

The reader will immediately note that (2) generalizes the foundation schema: Foundation is just the formal translation of the phrase "the (relation) $\in$ – i.e., $\{\langle x, y\rangle : y \in x\}$ where the "$\in$" in "$\{\ldots\}$" is the nonlogical predicate of $L_{\mathrm{Set}}$ – has MC".

This discussion is also meant to caution that the casualness of Definition VI.1.22 does *not* hide between the lines quantification over a class term ($\mathbb{A}$) – a thing we are not allowed to do.

Clearly, $\emptyset$ has MC. So, every relation can be "cut down" to a point that it has MC (if necessary, cut it down all the way to $\emptyset$). One interesting way to cut down a relation is by the process of restriction.

We say that $\mathbb{P}$ *has MC over* $\mathbb{A}$ just in case $\mathbb{P} \mid \mathbb{A}$ has MC.

The term "PO set" (also "poset") is standard. "LO set" is not much in circulation, but "WO set" has occurred elsewhere (Jech (1978b)). By analogy we have introduced the (non-standard) nomenclature PO class, LO class, and WO class. □

**VI.1.24 Proposition.** *The condition* "$\mathbb{P}$ has MC over $\mathbb{A}$" *is provably equivalent to*[‡]

$$\emptyset \neq \mathbb{B} \subseteq \mathbb{A} \to (\exists x \in \mathbb{B})\mathbb{B} \cap \mathbb{P}\langle x\rangle = \emptyset \tag{1}$$

*Proof.* Using the deduction theorem, we have two directions to prove:

→: Let us first *assume* that $\mathbb{P}$ has MC over $\mathbb{A}$. This means that $\mathbb{P} \mid \mathbb{A}$ has MC (by definition, VI.1.23), and therefore our assumption amounts to adding

[†] Here $x \in \mathbb{A}$; thus $\mathbb{P} \mid \mathbb{A}\langle x\rangle = \mathbb{A} \cap \mathbb{P}\langle x\rangle$ – see VI.1.21. A provable *schema* is, of course, one such that all its instances are (here, ZFC) theorems.

[‡] Where "$\emptyset \neq \mathbb{B} \subseteq \mathbb{A}$" is short for "$\emptyset \neq \mathbb{B} \wedge \mathbb{B} \subseteq \mathbb{A}$", i.e., utilizing the connectives "$\neq$" and "$\subseteq$" conjunctionally.

the schema below (cf. VI.1.23):

$$\emptyset \neq \mathbb{B} \to (\exists x \in \mathbb{B})\mathbb{B} \cap (\mathbb{P} \mid \mathbb{A}\langle x \rangle) = \emptyset \tag{1$a$}$$

Next, we focus on *one* unspecified $\mathbb{B}$ (so-called "arbitrary"). Now, after adding $\mathbb{B} \neq \emptyset$ and $\mathbb{B} \subseteq \mathbb{A}$, (1$a$) yields

$$(\exists x \in \mathbb{B})\mathbb{B} \cap \mathbb{P}\langle x \rangle = \emptyset$$

using Remark VI.1.21. This proves (1).

$\leftarrow$: Conversely, assume (add) (1), fix $\mathbb{B}$, and let $\emptyset \neq \mathbb{B}$ (it is *not* assumed that $\mathbb{B} \subseteq \mathbb{A}$).

We want to prove

$$(\exists x \in \mathbb{B})\mathbb{B} \cap (\mathbb{P} \mid \mathbb{A}\langle x \rangle) = \emptyset \tag{2}$$

*Case* $\mathbb{B} \cap \mathbb{A} = \emptyset$. Then

$$x \in \mathbb{B} \to \mathbb{B} \cap \big(\mathbb{A} \cap \mathbb{P}\langle x \rangle\big) = \emptyset$$

Therefore

$$x \in \mathbb{B} \to \mathbb{B} \cap (\mathbb{P} \mid \mathbb{A}\langle x \rangle) = \emptyset$$

by VI.1.21, which yields (2) by $\exists$-monotonicity (I.4.23) and modus ponens.

*Case* $\mathbb{B} \cap \mathbb{A} \neq \emptyset$. By (1),

$$(\exists x \in \mathbb{B} \cap \mathbb{A})(\mathbb{B} \cap \mathbb{A}) \cap \mathbb{P}\langle x \rangle = \emptyset \tag{3}$$

since $\mathbb{B} \cap \mathbb{A} \subseteq \mathbb{A}$. Therefore (2) is deduced again, since $(\mathbb{B} \cap \mathbb{A}) \cap \mathbb{P}\langle x \rangle = \mathbb{B} \cap (\mathbb{P} \mid \mathbb{A}\langle x \rangle)$ and the quantification in (3) can be changed to $(\exists x \in \mathbb{B})$.

Thus under both cases, the assumption $\emptyset \neq \mathbb{B}$ yields (2), i.e., $\mathbb{P}$ has MC over $\mathbb{A}$. □

**VI.1.25 Corollary.** *That $\mathbb{P}$ has MC over $\mathbb{A}$ is provably equivalent to the schema* (4) *below:*

$$(\exists x \in \mathbb{A})\mathscr{F}[x] \to (\exists x \in \mathbb{A})\big(\mathscr{F}[x] \wedge \neg(\exists y \in \mathbb{A})(y \,\mathbb{P}\, x \wedge \mathscr{F}[y])\big) \tag{4}$$

*Proof.* (a) Add schema (1) above, and prove schema (4): Fix $\mathscr{F}$, and let $\mathbb{B} = \mathbb{A} \cap \{x : \mathscr{F}[x]\}$. We add

$$(\exists x \in \mathbb{A})\mathscr{F}[x] \qquad \text{(hypothesis of (4))} \tag{5}$$

(5) yields $\emptyset \neq \mathbb{B} \subseteq \mathbb{A}$; hence, by (1),

$$(\exists x \in \mathbb{B})\mathbb{B} \cap \mathbb{P}\langle x \rangle = \emptyset \tag{6}$$

(6) yields

$$(\exists x \in \mathbb{B})\neg(\exists y)(y \,\mathbb{P}\, x \wedge y \in \mathbb{B})$$

which in turn yields

$$(\exists x \in \mathbb{A})\big(\mathscr{F}[x] \wedge \neg(\exists y \in \mathbb{A})(y \,\mathbb{P}\, x \wedge \mathscr{F}[y])\big)$$

This concludes the proof of (4).

(b) Conversely, assume (4) and prove (1): So let $\emptyset \neq \mathbb{B} \subseteq \mathbb{A}$ for fixed $\mathbb{B}$. The class $\mathbb{B}$ is "given" by a class term $\{x : \mathscr{B}[x]\}$, so that the assumption yields

$$(\exists x \in \mathbb{A})\mathscr{B}[x]$$

By (4) we get

$$(\exists x \in \mathbb{A})\big(\mathscr{B}[x] \wedge \neg(\exists y \in \mathbb{A})(y \,\mathbb{P}\, x \wedge \mathscr{B}[y])\big)$$

which, in terms of $\mathbb{B}$, reads

$$(\exists x \in \mathbb{A} \cap \mathbb{B})\mathbb{A} \cap \mathbb{P}\langle x\rangle \cap \mathbb{B} = \emptyset$$

which, in view of $\mathbb{B} \subseteq \mathbb{A}$, yields exactly what we want:

$$(\exists x \in \mathbb{B})\mathbb{B} \cap \mathbb{P}\langle x\rangle = \emptyset$$ □

**VI.1.26 Corollary.** *If $\mathbb{P}$ has MC over $\mathbb{A}$ and $\mathbb{B} \subseteq \mathbb{A}$, then $\mathbb{P}$ has MC over $\mathbb{B}$.*

*Proof.* By VI.1.24 we add the schema

$$\emptyset \neq \mathbb{C} \subseteq \mathbb{A} \to (\exists x \in \mathbb{C})\mathbb{C} \cap \mathbb{P}\langle x\rangle = \emptyset \tag{7}$$

and fix $\mathbb{A}$ and $\emptyset \neq \mathbb{D} \subseteq \mathbb{B} \subseteq \mathbb{A}$. We want

$$(\exists x \in \mathbb{D})\mathbb{D} \cap \mathbb{P}\langle x\rangle = \emptyset$$

which we have by (7), since the hypothesis implies $\emptyset \neq \mathbb{D} \subseteq \mathbb{A}$. □

**VI.1.27 Example (Informal).** $(\mathbb{N}, <)$, where $<$ is the natural order, is a WO set. $(\mathbb{Z}, <)$ is not. Define next $\prec$ on $\mathbb{N}^{n+1}$ by

$$\langle \vec{x}_{n+1}\rangle \prec \langle \vec{y}_{n+1}\rangle \quad \text{iff} \quad x_1 < y_1 \wedge x_i = y_i \text{ for } i = 2, \ldots, n+1$$

where "$<$" denotes the natural order on $\mathbb{N}$. Then $(\mathbb{N}^{n+1}, \prec)$ is a PO set (but *not* a LO set) with MC.

Indeed, $\prec$ is irreflexive and transitive ($\langle \vec{x}_{n+1}\rangle \prec \langle \vec{y}_{n+1}\rangle \prec \langle \vec{z}_{n+1}\rangle$ means $x_1 < y_1 < z_1$ and $x_i = y_i = z_i$ for $i = 2, \ldots, n+1$; hence $\langle \vec{x}_{n+1}\rangle \prec \langle \vec{z}_{n+1}\rangle$); therefore it is an order. Note that $\langle \vec{x}_{n+1}\rangle$ and $\langle \vec{y}_{n+1}\rangle$ are non-comparable if $x_2 \neq y_2$.

For any $\emptyset \neq B \subseteq \mathbb{N}^{n+1}$ the minimal elements are $(n+1)$-tuples with *minimum* first component. □

## VI.2. Induction and Inductive Definitions

We have already seen the application of induction, both informally (over $\mathbb{N}$) and formally (over $\omega$), as well as inductive definitions both over $\mathbb{N}$ (in definitions – cf. Section I.2 for the justification of this metatheoretical tool) and over $\omega$. The purpose of this section is to study the "induction phenomenon" further, since these techniques are commonplace in set theory (and logic in general). We will see that $\mathbb{N}$ and $\omega$ do not hold a monopoly on inductive techniques and that we can do induction and inductive (or recursive) definitions over much more general, indeed "longer", sets than the natural numbers.

**VI.2.1 Informal Definition.** A relation $\mathbb{P}$ (not necessarily an order) satisfies the *inductiveness condition*, or has IC, iff for every class $\mathbb{A}$

$$(\forall x)(\mathbb{P}\langle x\rangle \subseteq \mathbb{A} \to x \in \mathbb{A}) \to (\forall x)x \in \mathbb{A} \tag{1}$$

holds. Formula schema (1) is called the $\mathbb{P}$-*induction schema*. □

**VI.2.2 Remark.** As in the case of MC (cf. VI.1.23), *operationally*, the phrases "$\mathbb{P}$ has IC" and "let $\mathbb{P}$ have IC" are *argot*, respectively, for "(schema) (1) is provable" and "add schema (1) (as an axiom schema)".

Once again, we remind the reader that we are *not* quantifying over $\mathbb{A}$ in VI.2.1 any more than we are quantifying over a formula $\mathscr{F}$ in the statement of the collection axiom.

Practically speaking, what the induction schema (1) enables is as follows: If we want to prove $x \in \mathbb{A}$ for the *free variable* $x$, and if we know of some relation $\mathbb{P}$ that has IC,[†] then our task can be helped by the additional hypothesis – known as the *induction hypothesis*, (I.H. for short) – $\mathbb{P}\langle x\rangle \subseteq \mathbb{A}$.

This technique proves $(\forall x)x \in \mathbb{A}$ *by* $\mathbb{P}$*-induction on (the variable)* $x$.

Of course, what we have outlined above in English is how to prove

$$\mathbb{P}\langle x\rangle \subseteq \mathbb{A} \to x \in \mathbb{A}$$

via the deduction theorem; the usual restrictions on the free variables of $\mathbb{P}\langle x\rangle \subseteq \mathbb{A}$ apply.

Now, when employed in work within ZFC, $\mathbb{A}$ is just an *argot* name for the class term $\{x : \mathscr{A}[x]\}$; thus the $\mathbb{P}$-induction schema (or principle), for any $\mathbb{P}$ that has IC, can be restated without class names as

$$(\forall x)\Big((\forall y)(y\,\mathbb{P}\,x \to \mathscr{A}[y]) \to \mathscr{A}[x]\Big) \to (\forall x)\mathscr{A}[x] \tag{1a}$$

[†] We "know" because we either proved or assumed schema (1).

or, in English (again invoking the deduction theorem with the usual restrictions): If $\mathbb{P}$ has IC, then to prove $(\forall x).\mathscr{A}[x]$ it suffices to prove $\mathscr{A}[x]$ with the help of an additional "axiom" (induction hypothesis): that $(\forall y)(y\,\mathbb{P}\,x \rightarrow \mathscr{A}[y])$ – with all the free variables of this "axiom" frozen.

An elegant way to say the same thing is that "the property $\mathscr{A}$ *propagates with* $\mathbb{P}$" in the sense that if all the ("values" of) $y$ that are "predecessors" of $x$ – i.e., $y\,\mathbb{P}\,x$ – have the property, then so does $x$.[†]

If $\mathbb{P}$ is an *order*, then (1) will be immediately recognized *in form*. It generalizes the well-known principle of *course-of-values induction*[‡] over $\mathbb{N}$. □

One can easily verify that $\emptyset$ has IC.[§] As in the case of the MC property, a relation can be "cut down" until it acquires IC. In particular, this may come about by the process of restriction.

**VI.2.3 Definition.** We say that $\mathbb{P}$ *has IC over* $\mathbb{A}$ just in case $\mathbb{P} \mid \mathbb{A}$ has IC. □

**VI.2.4 Proposition.** *That* $\mathbb{P}$ *has IC over* $\mathbb{A}$ *is provably equivalent to the following schema:*

$$(\forall x \in \mathbb{A})(\mathbb{A} \cap \mathbb{P}\langle x\rangle \subseteq \mathbb{B} \rightarrow x \in \mathbb{B}) \rightarrow (\forall x \in \mathbb{A})x \in \mathbb{B} \tag{2}$$

*Proof. Only-if part.* Assume that $\mathbb{P}$ has IC over $\mathbb{A}$, i.e., add the following schema:

$$(\forall x)(\mathbb{P} \mid \mathbb{A}\langle x\rangle \subseteq \mathbb{D} \rightarrow x \in \mathbb{D}) \rightarrow (\forall x)x \in \mathbb{D} \tag{3}$$

To prove (2), fix $\mathbb{B}$ and add

$$(\forall x \in \mathbb{A})(\mathbb{A} \cap \mathbb{P}\langle x\rangle \subseteq \mathbb{B} \rightarrow x \in \mathbb{B})$$

that is,

$$(\forall x)\big(x \notin \mathbb{A} \vee (\mathbb{A} \cap \mathbb{P}\langle x\rangle \subseteq \mathbb{B} \rightarrow x \in \mathbb{B})\big)$$

or, provably equivalently,[¶]

$$(\forall x)(\mathbb{P} \mid \mathbb{A}\langle x\rangle \subseteq \mathbb{B} \rightarrow x \in \mathbb{B} \cup \overline{\mathbb{A}}) \tag{4}$$

[†] Here we are just trying to employ some visually suggestive nomenclature, thus we are forgetting the "reality" that $y$ is an "output" of $\mathbb{P}$ on "input" $x$ and thus, in the intuition of cause and effect, it comes after $x$. We are simply concentrating on the *visual effect*: $y$ appears to the left of $x$ in the expression $y\,\mathbb{P}\,x$.

[‡] This is the name of the induction over $\mathbb{N}$ that takes the I.H. on $0, \ldots, n-1$ – rather than just on $n-1$ – in order to help the case for $n$. We have encountered this in a formal setting in Peano arithmetic in volume 1, Chapter II. See also Exercise V.1.

[§] This is hardly surprising, in view of VI.1.23 and VI.2.11 below.

[¶] $\overline{\mathbb{A}} = \mathbb{U}_M - \mathbb{A}$.

by VI.1.21. Since $\mathbb{P}\,|\,\mathbb{A}\langle x\rangle \subseteq \mathbb{B} \cup \overline{\mathbb{A}}$ implies $\mathbb{P}\,|\,\mathbb{A}\langle x\rangle \subseteq \mathbb{B}$ (by VI.1.21), (4) – via tautological implication followed by ∀-monotonicity (I.4.24) – finally yields

$$(\forall x)(\mathbb{P}\,|\,\mathbb{A}\langle x\rangle \subseteq \mathbb{B} \cup \overline{\mathbb{A}} \to x \in \mathbb{B} \cup \overline{\mathbb{A}})$$

which, by (3), proves $(\forall x)x \in \mathbb{B} \cup \overline{\mathbb{A}}$, that is, $(\forall x \in \mathbb{A})x \in \mathbb{B}$. This establishes (2).

*If part.* Assume (2), fix $\mathbb{B}$, and calculate:

$$\begin{aligned}
&(\forall x)(\mathbb{P}\,|\,\mathbb{A}\langle x\rangle \subseteq \mathbb{B} \to x \in \mathbb{B})\\
\leftrightarrow\ &\Big\langle \text{tautological equivalence and Leibniz rule} \Big\rangle\\
&(\forall x)\Big((x \in \mathbb{A} \to \mathbb{P}\,|\,\mathbb{A}\langle x\rangle \subseteq \mathbb{B} \to x \in \mathbb{B}) \wedge\\
&\qquad (x \notin \mathbb{A} \to \mathbb{P}\,|\,\mathbb{A}\langle x\rangle \subseteq \mathbb{B} \to x \in \mathbb{B})\Big)\\
\leftrightarrow\ &\Big\langle \text{distributing } \forall \text{ over } \wedge\text{, VI.1.21, and simplifying using Leibniz rule} \Big\rangle\\
&(\forall x \in \mathbb{A})(\mathbb{A} \cap \mathbb{P}\langle x\rangle \subseteq \mathbb{B} \to x \in \mathbb{B}) \wedge (\forall x)(x \notin \mathbb{A} \to x \in \mathbb{B})\\
\to\ &\Big\langle \text{using (2)} \Big\rangle\\
&(\forall x)(x \in \mathbb{A} \to x \in \mathbb{B}) \wedge (\forall x)(x \notin \mathbb{A} \to x \in \mathbb{B})\\
\leftrightarrow\ &\Big\langle \text{distributing } \forall \text{ over } \wedge \Big\rangle\\
&(\forall x)\Big((x \in \mathbb{A} \to x \in \mathbb{B}) \wedge (x \notin \mathbb{A} \to x \in \mathbb{B})\Big)\\
\leftrightarrow\ &\Big\langle \text{tautological equivalence and Leibniz rule} \Big\rangle\\
&(\forall x)x \in \mathbb{B}
\end{aligned}$$

Thus, the top line implies the bottom line, as we need. □

The practical outcome is this: To prove $x \in \mathbb{A} \to x \in \mathbb{B}$ – i.e., to prove that $\mathbb{A} \subseteq \mathbb{B}$ – one normally applies the deduction theorem, freezing the free variables and assuming $x \in \mathbb{A}$. The aim is then to prove $x \in \mathbb{B}$ instead. Now, VI.2.4 shows that if we know of some relation $\mathbb{P}$ that has IC over $\mathbb{A}$, then we can use an additional hypothesis (I.H.), namely,

$$\mathbb{A} \cap \mathbb{P}\langle x\rangle \subseteq \mathbb{B}$$

Of course, an additional hypothesis usually helps.

**VI.2.5 Corollary.** *That $\mathbb{P}$ has IC over $\mathbb{A}$ is provably equivalent to the following schema:*

$$(\forall x \in \mathbb{A})\big((\forall y \in \mathbb{A})(y \,\mathbb{P}\, x \to \mathscr{F}[y]) \to \mathscr{F}[x]\big) \to (\forall x \in \mathbb{A})\mathscr{F}[x]$$

**VI.2.6 Remark.** In the above corollary $(\forall y \in \mathbb{A})(y \,\mathbb{P}\, x \to \mathscr{F}[y])$ is, of course, the I.H. The following formula is the *induction step*:

$$(\forall y \in \mathbb{A})(y \,\mathbb{P}\, x \to \mathscr{F}[y]) \to \mathscr{F}[x] \tag{$a$}$$

What happened to our familiar (from "ordinary" induction over $\mathbb{N}$, or $\omega$) *basis* step? The answer is that to prove the induction step $(a)$ with $x$ free entails that the proof must be valid, in particular, for *all* the $\mathbb{P}$-minimal elements of $\mathbb{A}$, if any.[†]

Now, when considering the case where $x$ is $\mathbb{P}$-minimal in $\mathbb{A}$, $(a)$ is provably equivalent to $\mathscr{F}[x]$ – which is a[‡] *basis* case for $x$: Instead of proving $(a)$, prove $\mathscr{F}[x]$.

Indeed, that $\mathscr{F}[x]$ implies $(a)$ is trivial. Conversely, since $y \in \mathbb{A} \wedge y \,\mathbb{P}\, x$ is *refutable* for an $x$ that we have assumed to be $\mathbb{P}$-minimal, $(\forall y)\big(y \in \mathbb{A} \wedge y \,\mathbb{P}\, x \to \mathscr{F}[y]\big)$ is provable, so that, if $(a)$ is, so is $\mathscr{F}[x]$ by modus ponens. □

**VI.2.7 Example (Informal).** The "course-of-values $<$-induction" over $\mathbb{N}$, as it is outlined in the elementary literature (e.g., discrete mathematics texts), says that to prove $(\forall n \in \mathbb{N})\mathscr{P}(n)$ one only need do (1) and (2) below:

$$\text{prove } \mathscr{P}(0) \tag{1}$$

and

$$\text{prove for every } n \in \mathbb{N} - \{0\} \text{ that } (\forall m < n)\mathscr{P}(m) \text{ implies } \mathscr{P}(n) \tag{2}$$

Stating (1) explicitly is standard folklore, but, as we have already remarked in VI.2.6 above, we can actually merge (1) and (2) into

$$(\forall n \in \mathbb{N})\big((\forall m < n)\mathscr{P}(m) \to \mathscr{P}(n)\big)$$

□

**VI.2.8 Remark.** In practice, Corollary VI.2.5 is often applied in such a way that the "verification" on the $\mathbb{P}$-minimal elements of $\mathbb{A}$ is stated and performed explicitly:

*Basis cases*: One proves $\mathscr{F}[x]$ *on the assumption* that $x \in \mathbb{A}$ is $\mathbb{P}$-minimal.

*Induction step*: One proves $\mathscr{F}[x]$ *on the assumption* that $x \in \mathbb{A}$ is *not* minimal, using as I.H. that $(\forall y \in \mathbb{A})(y \,\mathbb{P}\, x \to \mathscr{F}[y])$.

[†] It turns out that $\mathbb{P}$ has MC over $\mathbb{A}$, so that $\mathbb{A}$ does have minimal elements – Theorem VI.2.11 below.

[‡] "A" rather than "the", since there may be many minimal elements.

Of course, the usual precautions that one takes when applying the deduction theorem are taken. □

**VI.2.9 Definition.** For any relation $\mathbb{P}$, an *infinite descending* $\mathbb{P}$*-chain* is a function $f$ with the properties

(1) $\mathrm{dom}(f) = \omega$, and
(2) $(\forall n \in \omega) f(n+1)\, \mathbb{P}\, f(n)$. □

Intuitively, an infinite descending $\mathbb{P}$-chain is a sequence $a_0, a_1, \ldots$ such that $\ldots a_3\, \mathbb{P}\, a_2\, \mathbb{P}\, a_1\, \mathbb{P}\, a_0$.

**VI.2.10 Informal Definition.** A relation $\mathbb{P}$ is *well-founded* iff it has no infinite descending chains.

$\mathbb{P}$ is *well-founded over* $\mathbb{A}$ iff $\mathbb{P} \mid \mathbb{A}$ is well-founded. □

Intuitively, $\mathbb{P}$ is well-founded if the universe $\mathbb{U}_M$ cannot contain an infinite descending chain, while it is well-founded over $\mathbb{A}$ if $\mathbb{A}$ cannot contain an infinite descending chain. Clearly, no infinite descending $\mathbb{P}$-chain can start anywhere outside $\mathrm{dom}(\mathbb{P})$ in any case.

There is some disagreement on the term “well-founded”. In some of the literature it applies *definitionally* to what we have called relations “with MC”. However, in the presence of AC well-founded relations are precisely those that have MC, so the slight confusion – if any – is harmless.

**VI.2.11 Theorem.** *For any relation* $\mathbb{P}$ *the following are provable:*

(1) $\mathbb{P}$ *has MC over a class* $\mathbb{A}$ *iff it has IC over* $\mathbb{A}$.
(2) *If* $\mathbb{P}$ *has MC over* $\mathbb{A}$*, then* $\mathbb{P}$ *is well-founded over* $\mathbb{A}$.

*Proof.* (1): Consider the schema in VI.1.25 and the schema in VI.2.5. The former schema is that of MC over $\mathbb{A}$, while the latter is that of IC over $\mathbb{A}$. It is trivial to verify that an instance of any one of the two schemata realized with a formula $\mathscr{F}$ is provably equivalent to the contrapositive of the instance of the other realized with the formula $\neg\mathscr{F}$.

(2): Let instead $f$ be an infinite descending $\mathbb{P} \mid \mathbb{A}$-chain. Then $\emptyset \neq \mathrm{ran}(f) \subseteq \mathbb{A}$, and hence there is an $a \in \mathrm{ran}(f)$ which is $\mathbb{P} \mid \mathbb{A}$-minimal. Now, $a = f(n)$ for some $n \in \omega$, but $f(n+1)(\mathbb{P} \mid \mathbb{A}) f(n)$, contradicting the $\mathbb{P} \mid \mathbb{A}$-minimality of $a$. □

**VI.2.12 Corollary.** *If* $\mathbb{P}$ *has IC over* $\mathbb{A}$ *and* $\mathbb{B} \subseteq \mathbb{A}$*, then* $\mathbb{P}$ *has IC over* $\mathbb{B}$.

*Proof.* By VI.1.26. □

**VI.2.13 Corollary.** *Let $A$ be set. Then the following are provably equivalent:*

(1) $\mathbb{P}$ *has MC over $A$.*
(2) $\mathbb{P}$ *has IC over $A$.*
(3) $\mathbb{P}$ *is well-founded over $A$.*

*Proof.* We only need to prove that (3) implies (1). So assume (3), and let (1) fail. Let $\emptyset \neq B \subseteq A$ such that $B$ has no $\mathbb{P}$-minimal elements. Pick an $a \in B$. Since it cannot be $\mathbb{P}$-minimal, pick an $a_1 \in B$ such that $a_1 \mathbin{\mathbb{P}} a$. Since $a_1$ cannot be $\mathbb{P}$-minimal, pick an $a_2 \in B$ such that $a_2 \mathbin{\mathbb{P}} a_1$.

This process can continue *ad infinitum* to yield an infinite descending chain $\ldots a_3 \mathbin{\mathbb{P}} a_2 \mathbin{\mathbb{P}} a_1 \mathbin{\mathbb{P}} a$ in $A$, contradicting (3).

This argument used AC, and more formally it goes like this: Let $g$ be a choice function for $\mathbf{P}(B) - \{\emptyset\}$.[†] Define $f$ on $\omega$ by recursion as

$$f(n) = \begin{cases} g(B) & \text{if } n = 0 \\ g\big(B \cap \mathbb{P}\langle f(n-1)\rangle\big) & \text{if } n > 0 \end{cases}$$

$f$ is total on $\omega$ for $B \cap \mathbb{P}\langle f(n-1)\rangle \neq \emptyset$ for all $n > 0$, by assumption (cf. VI.1.24). By $g(x) \in x$ for all $x \in \mathbf{P}(B) - \{\emptyset\}$, we have $f(n) \in \mathbb{P}\langle f(n-1)\rangle$, i.e., $f(n)\mathbb{P}f(n-1)$ for all $n > 0$; thus $f$ is an infinite descending chain. □

**VI.2.14 Remark.** The corollary goes through for any class $\mathbb{A}$, not just a set $A$, as we will establish later.

It is also noted that a weaker version of AC was used in the proof, the so-called *axiom of dependent choices*, namely that "if $\mathbb{P}$ is a relation and $B \neq \emptyset$ a set such that $(\forall x \in B)(\exists y \in B) y \mathbin{\mathbb{P}} x$, then there is a total function $f : \omega \to B$ such that $(\forall n \in \omega) f(n+1) \mathbin{\mathbb{P}} f(n)$." □

**VI.2.15 Example.** If $\mathbb{P}$ is well-founded, then it is irreflexive. Indeed, if $a \mathbin{\mathbb{P}} a$ for some $a$, then $\lambda n.a$ on $\omega$ is an infinite descending chain $(\ldots a \mathbin{\mathbb{P}} a \mathbin{\mathbb{P}} a \mathbin{\mathbb{P}} a)$.

By Theorem VI.2.11, if $\mathbb{P}$ has IC (equivalently MC), then it is irreflexive.

If $\mathbb{P}$ is irreflexive but *not* well-founded, is then $\mathbb{P}^+$ a partial order? (A legitimate question, since $\mathbb{P}^+$ is transitive.) Well, no, for consider $R = \{\langle 1, 2\rangle, \langle 2, 3\rangle, \langle 3, 1\rangle\}$, which is irreflexive. Now $R^+ = \{\langle 1, 1\rangle, \langle 2, 2\rangle, \langle 3, 3\rangle, \langle 1, 2\rangle, \langle 2, 3\rangle, \langle 3, 1\rangle, \langle 1, 3\rangle, \langle 2, 1\rangle, \langle 3, 2\rangle\}$, which is *not* a partial order (it is reflexive), *nor* the reflexive closure of one, since it is not antisymmetric (e.g., $1 \mathbin{R} 3 \wedge 3 \mathbin{R} 1$ requires $1 = 3$).

It turns out that if $\mathbb{P}$ has MC, then so does $\mathbb{P}^+$, and hence, in particular, it is a partial order, being irreflexive. □

[†] Proof by auxiliary constant, "$g$".

**VI.2.16 Theorem.** *If $\mathbb{P}$ has MC (IC), then so does $\mathbb{P}^+$.*

*Proof.* Let $\emptyset \neq \mathbb{A}$ and $a \in \mathbb{A}$ be $\mathbb{P}$-minimal, i.e.,

$$\mathbb{P}\langle a \rangle \uparrow \tag{1}$$

Suppose now that $b \, \mathbb{P}^+ \, a$ for some $b$. Then, for some $f$ with $\mathrm{dom}(f) = n \in \omega$ and $n > 2$ (why $n > 2$?), we have $f(0) = a$, $f(n-1) = b$, and $f(i) \, \mathbb{P} \, f(i-1)$ for $i = 1, \ldots, n-1$ (V.2.8 and V.2.24). In particular, $f(1) \, \mathbb{P} \, f(0)$, which contradicts (1). Therefore $a$ is also $\mathbb{P}^+$-minimal. □

**VI.2.17 Corollary.** *If $\mathbb{P}$ has MC (IC) over $\mathbb{A}$, then $(\mathbb{P} \mid \mathbb{A})^+$ has MC (IC).*

*Proof.* It is given that $\mathbb{P} \mid \mathbb{A}$ has MC (IC). By VI.2.16 $(\mathbb{P} \mid \mathbb{A})^+$ has MC (IC). □

We cannot sharpen the above to "$\mathbb{P}^+$ has MC (IC) *over* $\mathbb{A}$", for that means that $\mathbb{P}^+ \mid \mathbb{A}$ has MC. The latter is not true, though: Let $\mathbb{O}$ be the odd natural numbers, and $R$ be defined *on* $\mathbb{N}$ by $x \, R \, y$ iff $x = y + 1$; thus $R^+ = \, >$.

Now, $R$ has MC over $\mathbb{O}$ (for $R \mid \mathbb{O} = \emptyset$), yet $R^+$ does not, for $R^+ \mid \mathbb{O}$ has an infinite descending chain in $\mathbb{O}$:

$$\cdots > 7 > 5 > 3 > 1$$

In particular, we note from this example that $(\mathbb{P} \mid \mathbb{A})^+ \neq \mathbb{P}^+ \mid \mathbb{A}$ in general.

**VI.2.18 Example.** Let $\prec$ on $\omega$ be defined by $n \prec m$ iff $m = n + 1$. It is obvious that $\prec$ is well-founded; hence it has MC and IC by VI.2.13.

What is $\prec$-induction? For notational convenience let "$(\forall x)$" stand for "$(\forall x \in \omega)$". Thus, for any formula $\mathscr{F}(x)$,

$$(\forall n)\big((\forall x \prec n)\mathscr{F}(x) \to \mathscr{F}(n)\big) \to (\forall n)\mathscr{F}(n)$$

holds. In other words, if $\mathscr{F}(0)$ is proved [this is provably equivalent to $(\forall x \prec 0)\mathscr{F}(x) \to \mathscr{F}(0)$ – see VI.2.6] and if also $\mathscr{F}(n-1) \to \mathscr{F}(n)$ is proved under the assumption $n > 0$, then $(\forall n)\mathscr{F}(n)$ is proved.

This is just our familiar "simple" (as opposed to "course-of-values") induction over $\omega$, stemming from the fact that $\omega$ is the smallest *inductive set* (see V.1.5 and V.1.6).

The "natural" $<$ on $\omega$ (i.e., $\in$) is $\prec^+$. $<$-induction over $\omega$ coincides with the course-of-values induction over $\omega$. □

**VI.2.19 Example.** We already know that the axiom of foundation yields that $\in$ has MC. Therefore properties of sets can be proved by $\in$-induction over $\mathbb{U}_M$. □

**VI.2.20 Example (Double Induction over $\omega$).** (See also Chapter V, p. 248.) We often want to prove

$$(\forall m)(\forall n)\mathscr{F}(m, n) \tag{1}$$

for some formula $\mathscr{F}$ and $m, n$ ranging over $\omega$. The obvious approach, which often works, is to do induction on, say, $m$ only, treating $n$ as a "parameter". That is (assuming the problem can be handled by "simple" induction):

(i) Prove $(\forall n)\mathscr{F}(0, n)$.
(ii) For $m \geq 0$ prove $(\forall n)\mathscr{F}(m+1, n)$ from the I.H. $(\forall n)\mathscr{F}(m, n)$.

Sometimes steps (i) and/or (ii) are not easy, and can be helped by induction on $n$, that is:

(iii) Prove $\mathscr{F}(0, 0)$.
(iv) For $n \geq 0$ prove $\mathscr{F}(0, n+1)$ from the I.H. (on $n$) $\mathscr{F}(0, n)$,

which settles (i) by induction on $n$, and then

(v) For $m \geq 0$ prove $\mathscr{F}(m+1, 0)$, from the I.H. of (ii) above.
(vi) For $m \geq 0, n \geq 0$ prove $\mathscr{F}(m+1, n+1)$ from the assumptions
   (a) I.H. on $n$, namely, $\mathscr{F}(m+1, n)$, and
   (b) I.H. on $m$ ((ii) above).

Let us revisit the above "cascaded" induction from a different point of view. Define $\prec$ on $\omega \times \omega$ by

$$\langle a, b\rangle \prec \langle c, d\rangle \quad \text{iff} \quad c = a + 1 \lor a = c \land d = b + 1$$

It is clear that $\prec$ is well-founded; hence it has IC over $\omega^2$.

What is the proof of (1) by $\prec$-induction?

(vii) Prove $\mathscr{F}(0, 0)$ ($\langle 0, 0\rangle$ is the unique $\prec$-minimal element in $\omega^2$) – this is step (iii).
(viii) For *non-minimal* $\langle m, n\rangle$ prove $\mathscr{F}(m, n)$ from the I.H. $\langle r, s\rangle \prec \langle m, n\rangle \to \mathscr{F}(r, s)$.

Item (viii) splits into the following cases:

- $m = 0$. Then prove $\mathscr{F}(0, n)$ from $\mathscr{F}(0, n-1)$ (why is $n > 0$?) – this is step (iv).
- $n = 0$. Then prove $\mathscr{F}(m, 0)$ from $(\forall n)\mathscr{F}(m-1, n)$ (why is $m > 0$?) – this is step (v).
- $m > 0,\ n > 0$.

Finally prove $\mathscr{F}(m, n)$ from $\mathscr{F}(m, n-1)$ and $(\forall n)\mathscr{F}(m-1, n)$ – this is step (vi). □

**VI.2.21 Example.** It is clear now that since sets such as $\omega - \{0\}$, $\mathbb{N} \cup \{-3, -2, -1\}$ are well-ordered (by $<$), we can carry induction proofs over them. In the former case the "basis" case is at 1; in the latter case it is at $-3$. □

We next turn to recursive (or inductive) definitions with respect to an arbitrary $\mathbb{P}$ that has IC: first one that is also an order, and then one that is not necessarily an order.

**VI.2.22 Definition (Left-Narrow Relations).** (Levy (1979).) A relation $\mathbb{P}$ is *left-narrow* iff $\mathbb{P}\langle x\rangle$ is a set for all $x$. It is *left-narrow over* $\mathbb{A}$ iff $\mathbb{P} \mid \mathbb{A}$ is left-narrow.

Left-narrow relations are also called *set-like* (Kunen (1980)). □

**VI.2.23 Example.** $\in$ is left-narrow, while $\ni$ is not. □

**VI.2.24 Definition (Segments).** If $<$ is an order on $\mathbb{A}$ and $a \in \mathbb{A}$, then the class $< \langle a\rangle$ is called the (initial) *segment* defined by $a$, while the class $\le \langle a\rangle$ is called the *closed* segment defined by $a$. □

$\le$ is $r_{\mathbb{A}}(<)$, of course, so that $\le \langle a\rangle =< \langle a\rangle \cup \{a\}$. Segments of left-narrow relations are sets.

**VI.2.25 Theorem (Recursive or Inductive Definitions).** *Let* $<: \mathbb{A} \to \mathbb{A}$ *be a left-narrow order with IC, and* $\mathbb{G}$ *a* (not necessarily total) *function* $\mathbb{G} : \mathbb{A} \times \mathbb{U}_M \to \mathbb{X}$ *for some class* $\mathbb{X}$. *Then there exists a unique function* $\mathbb{F} : \mathbb{A} \to \mathbb{X}$ *satisfying:*

$$(\forall a \in \mathbb{A})\mathbb{F}(a) \simeq \mathbb{G}(a, \mathbb{F} \restriction < \langle a\rangle) \tag{1}$$

The requirement of left-narrowness guarantees (with the help of collection; cf. III.11.28) that the second argument of $\mathbb{G}$ in (1) is a set. This restriction does not adversely affect applicability of the theorem, as the reader will be able to observe in the sequel.

Also recall that "$\simeq$" is Kleene's *weak equality*, so that in the recurrence (1) above we have either both sides defined and equal (as sets or atoms), or both undefined (see III.11.17).

*Proof.* The proof is essentially the same as that for recursive definitions over an inductively defined set that we carried out in the metatheory in I.2.13. See also the proof of V.1.21.

We prove uniqueness first, so let $\mathbb{H} : \mathbb{A} \to \mathbb{X}$ also satisfy (1). Let $a \in \mathbb{A}$, and adopt the I.H. that

$$(\forall b < a)\mathbb{F}(b) \simeq \mathbb{H}(b)$$

that is, $b < a \to (\forall y)(\langle b, y\rangle \in \mathbb{F} \leftrightarrow \langle b, y\rangle \in \mathbb{H})$, and therefore

$$\mathbb{F} \restriction < \langle a\rangle = \mathbb{H} \restriction < \langle a\rangle$$

It follows that (writing "$\simeq$" conjunctionally)

$$\begin{aligned}\mathbb{F}(a) &\simeq \mathbb{G}(a, \mathbb{F} \restriction < \langle a\rangle)\\ &\simeq \mathbb{G}(a, \mathbb{H} \restriction < \langle a\rangle)\\ &\simeq \mathbb{H}(a)\end{aligned}$$

This settles the claim of uniqueness: $(\forall a \in \mathbb{A})\mathbb{F}(a) \simeq \mathbb{H}(a)$, that is, $\mathbb{F} = \mathbb{H}$. Define now

$$\begin{aligned}\mathbb{K} = \big\{f : (\exists a \in \mathbb{A})\big(f :\leq \langle a\rangle \to \mathbb{X}\\ \wedge \big(\forall x \in \leq \langle a\rangle\big) f(x) \simeq \mathbb{G}(x, f \restriction < \langle x\rangle)\big)\big\}\end{aligned} \tag{2}$$

"$f :\leq \langle a\rangle \to \mathbb{X}$" stands for "$f$ is a function $\leq \langle a\rangle \to \mathbb{X}$". Thus, of course, in particular, $f$ is a class (not an atom). By left narrowness and III.11.28, any such $f$ is actually a set, so we *can* "define" the class term $\mathbb{K}$.

A classless way of stating (2) is to let $\mathbb{A} = \{x : \mathscr{A}(x)\}$, $\mathbb{G} = \{\langle\langle x, y\rangle, z\rangle : \mathscr{G}(x, y, z)\}$, and $\mathbb{X} = \{x : \mathscr{X}(x)\}$, adding the assumptions

$$\mathscr{G}(x, y, z) \to \mathscr{A}(x) \wedge \mathscr{X}(z)$$

and

$$\mathscr{G}(x, y, z) \wedge \mathscr{G}(x, y, z') \to z = z'$$

We then simply *name* the formula below "$\mathscr{M}(f, a)$", and let $\mathbb{K} = \{f : (\exists a)\,\mathscr{M}(f, a)\}$.

$$\begin{aligned}\neg U(f) \wedge \mathscr{A}(a) \wedge (\forall z)\big(z \in f \to OP(z) \wedge \pi(z) \leq a \wedge \mathscr{X}(\delta(z))\big)\\ \wedge (\forall x)(\forall y)(\forall z)(zfx \wedge yfx \to y = z)\\ \wedge \big(\forall x \in \leq \langle a\rangle\big)(\forall y)\big(yfx \leftrightarrow \mathscr{G}(x, \{\langle u, v\rangle : vfu \wedge u < x\}, y)\big)\end{aligned} \tag{2'}$$

In the formal description of $\mathbb{K}$ (i.e., (2′)) we have added the conjunct $\neg U(f)$ to exclude atoms. Informally we do not have to do this, since a function $f$ is a *class* (our only concern being whether it is proper or not).

We also note that $\mathbb{K} \neq \emptyset$. For example, if $a \in \mathbb{A}$ is $<$-minimal, then $\leq \langle a\rangle = \{a\}$, $< \langle a\rangle = \emptyset$, and hence $f \restriction < \langle a\rangle = \emptyset$ for any $f$; thus $\mathbb{K}$ contains $\{\langle a, \mathbb{G}(a, \emptyset)\rangle\}$ if $\mathbb{G}(a, \emptyset)\downarrow$, else it contains the empty function $\emptyset :\leq \langle a\rangle \to \mathbb{X}$. Indeed, for the latter we have $\emptyset(a) \simeq \mathbb{G}(a, \emptyset \restriction < \langle a\rangle)$, since both sides are undefined.

Since the uniqueness argument above does not depend on the particular left field $\mathbb{A}$, but only on the fact that $<$ has IC over $\mathbb{A}$, the same proof of uniqueness applies to the case that the left field is $\leq \langle a\rangle$ (a subset of $\mathbb{A}$),[†] showing that

$$\vdash_{\text{ZFC}} \mathscr{M}(f, a) \wedge \mathscr{M}(g, a) \rightarrow f = g \tag{3}$$

We have at once[‡]

$$\vdash_{\text{ZFC}} \mathscr{M}(f, a) \rightarrow \mathscr{M}(g, b) \rightarrow f(x) \downarrow \rightarrow g(x) \downarrow \rightarrow f(x) = g(x) \tag{3$'$}$$

because $\leq \langle x\rangle \subseteq \leq \langle a\rangle \cap \leq \langle b\rangle$ by transitivity;[§] hence $f \restriction \leq \langle x\rangle = g \restriction \leq \langle x\rangle$ by (3).

Now

$$\mathbb{F} = \bigcup \mathbb{K} \text{ is a function } \mathbb{F} : \mathbb{A} \rightarrow \mathbb{X} \tag{4}$$

for

$$\vdash \mathbb{F}(x) = y \leftrightarrow (\exists f)(\exists a)(\mathscr{M}(f, a) \wedge f(x) = y)$$

Thus, if $\mathbb{F}(x) = y$ and $\mathbb{F}(x) = z$, then (using auxiliary constants $f, g, a, b$) we add

$$f(x) = y \wedge \mathscr{M}(f, a) \tag{5}$$

and

$$g(x) = z \wedge \mathscr{M}(g, b) \tag{6}$$

from which (and (3$'$)) we derive $y = z$.

In preparation for our final step we note that

$$\vdash_{\text{ZFC}} \mathscr{M}(f, a) \rightarrow f = \mathbb{F} \restriction \leq \langle a\rangle \tag{7}$$

Assume the hypothesis, and let $x \leq a$. Then, $f(x) = y$ implies $\mathbb{F}(x) = y$ by (4). Conversely, under the same hypotheses – $\mathscr{M}(f, a)$ and $x \leq a$ – assume also $\mathbb{F}(x) = z$. This leads (say, via new constants $g$ and $b$) to (6). Since $x \in \leq\langle a\rangle \cap \leq\langle b\rangle$, we get $f(x) = g(x) = \mathbb{F}(x)$ (cf. footnote related to (3$'$)).

We finally verify that $\mathbb{F}$ satisfies the recurrence (1) of the theorem. Indeed, let $\mathbb{F}(x) = y$, which, using auxiliary constants $f$ and $a$, leads to the assumption (5)

[†] Of course, $<$ has IC over $\leq \langle a\rangle$ for any $a \in \mathbb{A}$ (cf. VI.2.12).

[‡] We do mean "=" rather than the wishy-washy "$\simeq$" here, since $x \in \text{dom}(f) \cap \text{dom}(g)$. Note that if we had known that $x \in \leq \langle a\rangle \cap \leq \langle b\rangle$, then only one of the hypotheses $f(x) \downarrow$ or $g(x) \downarrow$ would have sufficed.

[§] We have just used the assumption that $<$ is an order.

above. Then, by $\mathscr{M}(f, a)$ – specifically, specializing the last conjunct of (2′) – we get

$$\mathscr{G}(x, \{\langle u, v\rangle : v\ f\ u\ \wedge u < x\}, y)$$

Hence,

$$\mathscr{G}(x, \{\langle u, v\rangle : v\,\mathbb{F}\,u \wedge u < x\}, y)$$

by (7). That is,

$$\vdash_{\mathrm{ZFC}} \mathbb{F}(x) = y \to \mathbb{G}(x, \mathbb{F} \restriction< \langle x\rangle) = y$$

We now want the converse,

$$\vdash_{\mathrm{ZFC}} \mathbb{G}(x,\ \mathbb{F} \restriction< \langle x\rangle) = y \to \mathbb{F}(x) = y \tag{8}$$

Let $a \in \mathbb{A}$ be $<$-minimal for which (8) fails. This failure means that we have

$$\mathbb{G}(a, \mathbb{F} \restriction< \langle a\rangle) = b \qquad \text{for some appropriate } b \in \mathbb{X} \tag{9}$$

yet[†]

$$\mathbb{F}(a) \uparrow \tag{10}$$

We define $h = \mathbb{F} \restriction< \langle a\rangle$ (a renaming of convenience), which is a function. By minimality of $a$, the function $\mathbb{F}$, and hence $h$, satisfy the recurrence (1) on $< \langle a\rangle$, that is

$$(\forall x \in< \langle a\rangle) h(x) \simeq \mathbb{G}(x, h \restriction< \langle x\rangle) \tag{11}$$

The function $f = h \cup \{\langle a, b\rangle\}$ satisfies $(\forall x \in\leq \langle a\rangle) f(x) \simeq \mathbb{G}(x, f \restriction< \langle x\rangle)$, because of (9). Hence $f \subseteq \mathbb{F}$ by (4). Now, $f(a) = b$ contradicts (10). □

**VI.2.26 Remark.** (1) Pretending that the above proof took place in the metatheory, one can view it as "constructively" demonstrating the "existence" of a class $\mathbb{F}$ with the stated properties. Formally, we *cannot* quantify over classes. Thus, to prove "$(\forall\mathbb{A})\ldots\mathbb{A}\ldots$" one proves the *schema* "$\ldots\mathbb{A}\ldots$" for the arbitrary $\mathscr{A}$ (that "defines" $\mathbb{A} = \{x : \mathscr{A}\}$). To prove "$(\exists\mathbb{A})\ldots\mathbb{A}\ldots$" one must exhibit a *specific formula* $\mathscr{A}$ (that gives rise to $\mathbb{A}$ as above) for which we can prove (the formal translation of) "$\ldots\mathbb{A}\ldots$".

In particular, what we really did in the above proof were two things:

(a) We stated a *formula* $\mathscr{F}(x, y)$, displayed below, that was built from given formulas:

$$(\exists f)(\exists a)(\mathscr{M}(f, a) \wedge \langle x, y\rangle \in f)$$

where $\mathscr{M}$ is given by (2′). We then *proved the theorems*

$$\mathscr{F}(x, y) \wedge \mathscr{F}(x, y') \to y = y' \tag{$*$}$$

[†] Clearly, by the direction already proved, $\mathbb{F}(a) \downarrow$ is incompatible with the failure of (8).

and (1) of the theorem, using in the latter case the abbreviation $\mathbb{F}(x) = y$ for $\mathscr{F}(x, y)$. This was our "existence" proof.

The reader will have absolutely no trouble verifying that if instead of $\mathbb{G}$ we have a *function symbol*, $\boldsymbol{G}$, of arity 2, and a relation $<$ with IC (dropping $\mathbb{A}$ and $\mathbb{X}$), then we can introduce a function symbol of arity 1, $\boldsymbol{F}$, so that the following holds:

$$\vdash_{\mathrm{ZFC}} (\forall a)\boldsymbol{F}(a) = \boldsymbol{G}(a, \boldsymbol{F} \restriction_{<} \langle a\rangle)$$

Indeed, $\boldsymbol{F}$ can be introduced by

$$\boldsymbol{F}(x) = y \leftrightarrow (\exists f)(\exists a)(\mathscr{M}(f, a) \wedge f(x) = y) \tag{$**$}$$

since we can prove, under these assumptions,[†] that

$$\vdash_{\mathrm{ZFC}} (\forall x)(\exists! y)(\exists f)(\exists a)(\mathscr{M}(f, a) \wedge f(x) = y)$$

Even in the presence of an $\mathbb{A}$ we can always introduce $\boldsymbol{F}$ (using the techniques in III.2.4) by saying "under the assumption $x \in \mathbb{A}$, $(**)$ is derivable, while under the assumption $x \notin \mathbb{A}$, $\boldsymbol{F}(x) = \emptyset$ is derivable" (definition by cases). (See Exercise VI.5.)

(b) The uniqueness part showed that our "solution" $\mathscr{F}$ is unique within equivalence: Any other formula $\mathscr{H}$ that is functional (i.e., satisfies $(*)$ above with $\mathscr{F}$ replaced by $\mathscr{H}$) and "solves" (1)) is provably equivalent to $\mathscr{F}$:

$$\mathscr{A}(x) \to \big(\mathscr{F}(x, y) \leftrightarrow \mathscr{H}(x, y)\big)$$

The above discussion makes it clear that using class terminology and notation was a good idea.

(2) The recursion on the natural numbers (V.1.21) is a special case of VI.2.25: Indeed,

$$\begin{aligned} f(0) &= a \\ \text{for } n \geq 0,\ \ f(n+1) &= g(n, f(n)) \end{aligned}$$

can be rewritten as

$$\begin{aligned} (\forall n \in \omega) f(n) &\simeq G(n, f \restriction_{<} \langle n\rangle) \\ &\simeq G(n, f \restriction n) \end{aligned}$$

[†] $\mathbb{G}$ is obtained from $\boldsymbol{G}$ as in III.11.20. Conversely, starting with $\mathbb{G} = \{\langle\langle x, y\rangle, z\rangle : \mathscr{G}(x, y, z)\}$, a function, we have $\mathscr{G}(x, y, z) \to \mathscr{G}(x, y, z') \to z = z'$. We can then introduce $\boldsymbol{G}$ by $\boldsymbol{G}(x, y) = z \leftrightarrow \mathscr{G}(x, y, z)$.

where

$$G(n,h) = \begin{cases} a & \text{if } n = 0 \\ g(n-1, h(n-1)) & \text{if } h \text{ is a function} \wedge \mathrm{dom}(h) = n > 0 \\ \uparrow & \text{otherwise} \end{cases}$$

Note that $G$ on $\omega \times \mathbb{U}_M$ is nontotal. In particular, if the second argument is not of the correct type (middle case above), $G$ will be undefined. We can still prove that $f(n) \downarrow$ for all $n \in \omega$, without using V.1.21.

Assume the claim for $m < n$ (I.H.). For $n = 0$, we have $f(0) \simeq G(0, \emptyset) = a$, defined. Let next $n > 0$. Now $f(n) \simeq G(n, f \restriction n)$ and $\mathrm{dom}(f \restriction n) = n$ by I.H.; hence $f(n) = g(n-1, (f \restriction n)(n-1)) = g(n-1, f(n-1))$, defined, since $g$ is total.

(3) In view of the above, it is worth noting that a recursive definition *à la* VI.2.25 can still define a total function, even if $\mathbb{G}$ is nontotal. □

**VI.2.27 Corollary (Definition by Recursion with Respect to an Arbitrary Relation with IC[†]).** *Let* $\mathbb{P} : \mathbb{A} \to \mathbb{A}$ *be a left-narrow relation* – not necessarily an order – *with IC, and* $\mathbb{G}$ *a* (not necessarily total) *function* $\mathbb{G} : \mathbb{A} \times \mathbb{U}_M \to \mathbb{X}$ *for some class* $\mathbb{X}$*. Then there exists a unique function* $\mathbb{F} : \mathbb{A} \to \mathbb{X}$ *satisfying*

$$(\forall a \in \mathbb{A})\mathbb{F}(a) \simeq \mathbb{G}(a, \mathbb{F} \restriction \mathbb{P}\langle a \rangle)$$

*Proof.* Define $\widetilde{\mathbb{G}} : \mathbb{A} \times \mathbb{U}_M \to \mathbb{X}$ by

$$\widetilde{\mathbb{G}}(a, f) = \begin{cases} \emptyset & \text{if } f \text{ is not a function} \\ \mathbb{G}(a, f \restriction \mathbb{P}\langle a \rangle) & \text{otherwise} \end{cases}$$

Let $<$ stand for $\mathbb{P}^+$. Now $<$ is an order on $\mathbb{A}$ with IC by VI.2.16. Moreover it is left-narrow by the axiom of union, since (V.2.24)

$$\mathbb{P}^+\langle a \rangle = \bigcup \left\{ \mathbb{P}^n \langle a \rangle : n \in \omega - \{0\} \right\}$$

and an easy induction on $n$ shows that each $\mathbb{P}^n\langle a \rangle$ is a set (Exercise VI.2). Thus, by VI.2.25, there is a unique $\mathbb{F} : \mathbb{A} \to \mathbb{X}$ such that

$$\begin{aligned} (\forall a \in \mathbb{A})\mathbb{F}(a) &\simeq \widetilde{\mathbb{G}}(a, \mathbb{F} \restriction_< \langle a \rangle) \\ &\simeq \mathbb{G}\Big(a, \big(\mathbb{F} \restriction_< \langle a \rangle\big) \restriction \mathbb{P}\langle a \rangle\Big) \end{aligned} \tag{1}$$

Now, $\mathbb{P}\langle a \rangle \subseteq_< \langle a \rangle$ yields $(\mathbb{F} \restriction_< \langle a \rangle) \restriction \mathbb{P}\langle a \rangle = \mathbb{F} \restriction \mathbb{P}\langle a \rangle$; hence (1) becomes

$$(\forall a \in \mathbb{A})\mathbb{F}(a) \simeq \mathbb{G}(a, \mathbb{F} \restriction \mathbb{P}\langle a \rangle) \qquad \square$$

[†] This idea is due to Montague (1955) and Tarski (1955).

**VI.2.28 Corollary (Recursion with a Total $\mathbb{G}$).** *Let $\mathbb{P} : \mathbb{A} \to \mathbb{A}$ be a left-narrow relation – not necessarily an order – with IC, and $\mathbb{G}$ a total function $\mathbb{G} : \mathbb{A} \times \mathbb{U}_M \to \mathbb{X}$, for some class $\mathbb{X}$. Then there exists a unique total function $\mathbb{F} : \mathbb{A} \to \mathbb{X}$ satisfying*

$$(\forall a \in \mathbb{A})\mathbb{F}(a) = \mathbb{G}(a, \mathbb{F} \restriction \mathbb{P}\langle a\rangle)$$

*Proof.* We only need to show that $\mathrm{dom}(\mathbb{F}) = \mathbb{A}$. By VI.2.27, there is a *unique* $\mathbb{F}$ satisfying

$$(\forall a \in \mathbb{A})\mathbb{F}(a) \simeq \mathbb{G}(a, \mathbb{F} \restriction \mathbb{P}\langle a\rangle)$$

But the right hand side of $\simeq$ is defined for all $a \in \mathbb{A}$; thus we can use "=" instead of "$\simeq$" in the statement of VI.2.27. □

**VI.2.29 Corollary (Recursive Definition with Parameters I).** *Let $\mathbb{P} : \mathbb{A} \to \mathbb{A}$ be a left-narrow relation – not necessarily an order – with IC, and $\mathbb{G}$ a (not necessarily total) function $\mathbb{G} : \mathbb{S} \times \mathbb{A} \times \mathbb{U}_M \to \mathbb{X}$, for some classes $\mathbb{S}$ and $\mathbb{X}$. Then there* exists *a unique function $\mathbb{F} : \mathbb{S} \times \mathbb{A} \to \mathbb{X}$ satisfying*[†]

$$(\forall \langle s, a\rangle \in \mathbb{S} \times \mathbb{A})\mathbb{F}(s, a) \simeq \mathbb{G}(s, a, \{\langle s, x, \mathbb{F}(s, x)\rangle : x \,\mathbb{P}\, a\}) \tag{1}$$

In equation (1) $s$ persists throughout (unchanged); hence it is called a *parameter*.

*Proof.* Define the relation $\widetilde{\mathbb{P}}$ on $\mathbb{S} \times \mathbb{A}$ by

$$\langle u, a\rangle \,\widetilde{\mathbb{P}}\, \langle v, b\rangle \quad \text{iff} \quad u = v \wedge a \,\mathbb{P}\, b$$

It is clear that $\widetilde{\mathbb{P}}$ has MC. Now, (1) can be rewritten as

$$\begin{aligned}(\forall \langle s, a\rangle \in \mathbb{S} \times \mathbb{A})\mathbb{F}(s, a) &\simeq \mathbb{G}(s, a, \{\langle s, x, \mathbb{F}(s, x)\rangle : \langle s, x\rangle \,\widetilde{\mathbb{P}}\, \langle s, a\rangle\}) \\ &\simeq \mathbb{G}\big(s, a, \mathbb{F} \restriction \widetilde{\mathbb{P}}\big\langle\langle s, a\rangle\big\rangle\big)\end{aligned}$$

The result follows from VI.2.27 by using $\mathbb{J}$ given below as "$\mathbb{G}$-function":

$$\mathbb{J}(g, f) = \begin{cases} \uparrow & \text{if } g \notin \mathbb{S} \times \mathbb{A} \\ \mathbb{G}(\pi(g), \delta(g), f) & \text{otherwise} \end{cases}$$

□

[†] "$(\forall \langle s, a\rangle \in \mathbb{S} \times \mathbb{A})$" is *argot* for "$(\forall z)(OP(z) \wedge \pi(z) \in \mathbb{S} \wedge \delta(z) \in \mathbb{A} \to \ldots$", or, simply, "$(\forall s \in \mathbb{S})(\forall x \in \mathbb{A})$".

**VI.2.30 Corollary (Recursive Definition with Parameters II).** *Let all assumptions be as in Corollary* VI.2.29*, except that the recurrence now reads*

$$(\forall \langle s, a\rangle \in \mathbb{S} \times \mathbb{A})\mathbb{F}(s, a) \simeq \mathbb{G}(s, a, \{\langle x, \mathbb{F}(s, x)\rangle : x \,\mathbb{P}\, a\}) \tag{1}$$

*Then there exists a unique function* $\mathbb{F} : \mathbb{S} \times \mathbb{A} \to \mathbb{X}$ *satisfying* (1).

*Proof.* Apply Corollary VI.2.29 with a "$\mathbb{G}$-function", $\mathbb{J}$, given by

$$\mathbb{J}(s, a, f) = \mathbb{G}(s, a, p_{23}(f))$$

where $p_{23} : \mathbb{U}_M \to \mathbb{U}_M$ is

$$p_{23}(f) = \begin{cases} \uparrow & \text{if } f \text{ is } \textit{not} \text{ a class of 3-tuples} \\ \{\langle \delta(\pi(z)), \delta(z)\rangle : z \in f\} & \text{otherwise} \end{cases}$$

□

**VI.2.31 Corollary (*Pure* Recursion with Respect to a Well-Ordering and with a Partial $\mathbb{G}$).** *Let* $<: \mathbb{A} \to \mathbb{A}$ *be a left-narrow well-ordering, and* $\mathbb{G}$ *a (not necessarily total) function* $\mathbb{G} : \mathbb{U}_M \to \mathbb{X}$ *for some class* $\mathbb{X}$. *Then there exists a unique function* $\mathbb{F} : \mathbb{A} \to \mathbb{X}$ *satisfying* (1)–(2) *below:*

(1) $(\forall a \in \mathbb{A})\mathbb{F}(a) \simeq \mathbb{G}(\mathbb{F} \restriction < \langle a\rangle)$,
(2) $\mathrm{dom}(\mathbb{F})$ *is either* $\mathbb{A}$, *or* $< \langle a\rangle$ *for some* $a \in \mathbb{A}$.

"Pure recursion" refers to the fact that $\mathbb{G}$ has only one argument, the "history" of $\mathbb{F}$ on the segment $< \langle a\rangle$.

*Proof.* In view of Theorem VI.2.25, we need only prove (2). So let $\mathrm{dom}(\mathbb{F}) \neq \mathbb{A}$. Let $a$ in $\mathbb{A}$ be $<$-minimal (also *minimum* here, since $<$ is total) such that[†]

$$\mathbb{F}(a) \uparrow \quad \text{i.e.,} \quad \mathbb{G}(\mathbb{F} \restriction < \langle a\rangle) \uparrow \tag{3}$$

Thus $< \langle a\rangle \subseteq \mathrm{dom}(\mathbb{F})$. We will prove that $\mathrm{dom}(\mathbb{F}) =< \langle a\rangle$. Well, let instead $b \in \mathrm{dom}(\mathbb{F})- < \langle a\rangle$ be minimal.[‡]

By (3) and totalness of $<$, we have $a < b$. By choice of $b$,

$$(\forall x)(a \leq x \wedge x < b \to \mathbb{F}(x) \uparrow)$$

Thus,

$$\mathbb{F} \restriction < \langle b\rangle = \mathbb{F} \restriction < \langle a\rangle \tag{4}$$

[†] Proof by auxiliary constant hiding between the lines.
[‡] Another hidden proof by auxiliary constant.

Therefore

$$\begin{aligned}\mathbb{F}(b) &\simeq \mathbb{G}(\mathbb{F}\upharpoonright_{<\langle b\rangle})\\ &\simeq \mathbb{G}(\mathbb{F}\upharpoonright_{<\langle a\rangle}) \text{ (by (4))}\end{aligned}$$

contradicting (3), since $\mathbb{F}(b)\downarrow$. □

**VI.2.32 Example.** Let $G : 2 \times \mathbb{U} \to 2$ (recall that $2 = \{0, 1\}$) be

$$G(x, f) = \begin{cases} 1 & \text{if } x = 1 \wedge f = \emptyset \\ \uparrow & \text{otherwise} \end{cases}$$

and 2 be equipped with the "standard order" $<$ (i.e., $\in$) on $\omega$. Then the recursive definition

$$(\forall a \in 2) F(a) \simeq G(a, F\upharpoonright_{<\langle a\rangle})$$

yields the function $F = \{\langle 1, 1\rangle\}$, whose domain is neither 2 nor a segment of 2. Thus the requirement of *pure* recursion in VI.2.31 is essential.[†] □

**VI.2.33 Remark.** In practice, recursive definitions with respect to a $\mathbb{P}$ that has MC (IC) have often the form

$$\mathbb{F}(s, x) \simeq \begin{cases} \mathbb{H}(s) & \text{if } x \text{ is } \mathbb{P}\text{-minimal} \\ \mathbb{G}(s, x, \{\langle s, y, \mathbb{F}(s, y)\rangle : y\,\mathbb{P}\,x\}) & \text{otherwise} \end{cases}$$

This reduces to the case considered in VI.2.29 with a "$\mathbb{G}$-function" $\widetilde{\mathbb{G}}$ given by

$$\widetilde{\mathbb{G}}(s, x, f) = \begin{cases} \mathbb{H}(x) & \text{if } x \text{ is } \mathbb{P}\text{-minimal} \\ \mathbb{G}(s, x, f) & \text{otherwise} \end{cases}$$

A similar remark holds – regarding making the basis of the recursion explicit – for all the forms of recursion that we have considered. □

**VI.2.34 Example (The Support Function).** The *support* function $sp : \mathbb{U}_M \to \mathbb{U}_M$ gives the set of all urelements, $sp(x)$, that took part in the formation of some set $x$. For example,

$$\begin{aligned} sp(\emptyset) &= \emptyset \\ sp(n) &= \emptyset \quad \text{for every } n \in \omega \qquad \text{(induction on } n\text{)} \\ sp(\omega) &= \emptyset \\ sp(\{2, ?, \{\#, !, \omega\}\}) &= \{?, \#, !\} \qquad \text{for urelements } ?, \#, ! \end{aligned}$$

[†] Purity of recursion we tacitly took advantage of in the last step of the proof of VI.2.31. Imagine what would happen if $\mathbb{F}$'s argument were explicitly present in $\mathbb{G}$: We would get $\mathbb{G}(b, \mathbb{F}\upharpoonright_{<\langle b\rangle}) \simeq \mathbb{G}(b, \mathbb{F}\upharpoonright_{<\langle a\rangle})$, a dead end, since what we have is $\mathbb{G}(a, \mathbb{F}\upharpoonright_{<\langle a\rangle})\uparrow$, not $\mathbb{G}(b, \mathbb{F}\upharpoonright_{<\langle a\rangle})\uparrow$.

The existence and uniqueness of $sp$ is established by the following recursive definition:

$$sp(x) = \begin{cases} \{x\} & \text{if } x \text{ is an urelement} \\ \bigcup\{sp(y) : y \in x\} & \text{otherwise} \end{cases} \tag{1}$$

That (1) is an appropriate recursion can be seen as follows: First, $\in$ (the relation, not the predicate) is left-narrow and has MC. Next, (1) can be put in standard form (Corollary VI.2.28 in this case)

$$(\forall x \in \mathrm{dom}(sp))sp(x) = \mathbb{G}(x, sp \upharpoonright \in \langle x \rangle)$$

(of course, $\in \langle x \rangle = x$), where the *total* $\mathbb{G} : \mathbb{U}_M \times \mathbb{U}_M \to \mathbb{U}_M$ is given by

$$\mathbb{G}(x, f) = \begin{cases} \{x\} & \text{if } x \text{ is an urelement} \\ \emptyset & \text{otherwise, if } f \text{ is not a relation} \\ \bigcup \mathrm{ran}(f) & \text{in all other cases} \end{cases}$$

Note that in view of the discussion in Remark VI.2.26, we may introduce “$sp$” as a new formal function symbol. □

**VI.2.35 Definition (Pure Sets).** A set with empty support is called a *pure* set. □

**VI.2.36 Example (Mostowski’s Collapsing Function).** Here is another function on sets that is an important tool in the model theory of set theory. It is a function $C : \mathbb{U}_M \times \mathbb{U}_M \to \mathbb{U}_M$ defined by

$$C(p, x) = \begin{cases} x & \text{if } x \text{ is an urelement} \\ \{C(p, y) : y \in p \wedge y \in x\} & \text{otherwise} \end{cases} \tag{1}$$

This too can be introduced formally if desired (cf. VI.2.26). Note that $p$ is a parameter.

What does $C$ do – i.e., what is $C(p, x)$ – to a set or urelement $x$ in the context of the “reference” set or urelement $p$?

Well, if $x$ is an urelement, then $C$ does not change it. In the contrary case, if $p$ is an urelement, then $y \in p$ is refutable and thus $C(p, x) = \emptyset$.

The interesting subcase is when $p$ is a set. Suppose that $x \cap p = x' \cap p$ despite (possibly) $x \neq x'$. We get from (1)

$$C(p, x) = \{C(p, y) : y \in p \cap x\} = \{C(p, y) : y \in p \cap x'\} = C(p, x')$$

In other words, $C$ “collapses” any two sets $x$ and $x'$ *if their (possible) differences cannot be witnessed inside* $p$. That is, an inhabitant of $p$, aware only of members of $p$ but of nothing outside $p$, cannot tell $x$ and $x'$ apart on the basis of extensionality (trying to find *something in p* that is in one of $x$ or $x'$ but not in the other).

Here is a concrete example: Let $p = \{\#, !, ?, \{\#, @, ?\}, \{\#, ?\}\}$, where #, !, ?, @ are urelements, and let $x = \{\#, @, ?\}$ and $x' = \{\#, ?\}$. Now,

$$\begin{aligned}
C(p, \#) &= \# \\
C(p, !) &= ! \\
C(p, ?) &= ? \\
C(p, @) &= @ \\
C(p, x) &= \{C(p, y) : y \in p \cap x\} \\
&= \{C(p, y) : y = \# \vee y = ?\} = \{\#, ?\} \\
&= x'
\end{aligned}$$

while

$$\begin{aligned}
C(p, x') &= \{C(p, y) : y \in p \cap x'\} \\
&= \{C(p, y) : y = \# \vee y = ?\} = \{\#, ?\} \\
&= x'
\end{aligned}$$

and

$$\begin{aligned}
C(p, p) &= \{C(p, y) : y \in p\} \\
&= \{C(p, y) : y = \# \vee y =! \vee y = ? \vee y = x \vee y = x'\} \\
&= \{\#, !, ?, \{\#, ?\}\}
\end{aligned}$$

Note that – in the place of the two original $x$ and $x'$ of $p$ – $C(p, p)$ (the "collapsed $p$") only contains the common collapsed element, the set $C(p, x)$ $(= C(p, x'))$. Moreover, we note that the $C(p, p)$ that we have just computed is transitive. This is not a coincidence with the present $p$, but holds for all $p$:

Indeed, if $C(p, p)$ is not an atom (case where $p$ is an urelement), then it is a transitive set (why *set*?). To verify, let next $p$ be a set and (using conjunctional notation)

$$a \in b \in C(p, p) = \{C(p, x) : x \in p\} \tag{2}$$

Then $b = C(p, x)$ for some $x \in p$ (III.8.7). Now, one case is where $x$ is an urelement, hence $b = x$ (by (1)). Since $a \in b$ is now refutable, $a \in b \in C(p, p) \to a \in C(p, p)$ follows.

The other case leads to

$$b = \{C(p, y) : y \in p \cap x\}$$

By the assumption $a \in b$, $a = C(p, y)$ for some $y \in p \cap x \subseteq p$; hence (by (1)) $a \in C(p, p)$.

We conclude by putting the recursion (1) in standard form (that of Corollary VI.2.29 – hence $C$ is total on $\mathbb{U}_M^2$, since $\widetilde{\mathbb{G}}$ below is). Just take as "$\mathbb{G}$-function" $\widetilde{\mathbb{G}} : \mathbb{U}_M^3 \to \mathbb{U}_M$, given by

$$\widetilde{\mathbb{G}}(p, x, f) = \begin{cases} x & \text{if } x \text{ is an urelement} \\ \emptyset & \text{else, if } p \text{ is an atom} \\ \emptyset & \text{else, if } f \text{ is not a relation} \\ \operatorname{ran}(f \restriction (\{p\} \times (p \cap x))) & \text{in all other cases} \end{cases}$$

The reader will have no trouble putting future recursions in "standard" form, and we delegate to him all future instances of such an exercise. □

**VI.2.37 Remark.** What lies behind the fact that $C(p, p)$ is transitive, intuitively speaking? Well, by "squeezing out" those elements of $x$ (in $p$ – such as @ above) which do not help to establish the "identity" of $x$ in $p$, we have left in $x$, in essence, only those objects which (in squeezed form, of course) $p$ "knows about" (i.e., are its elements). The collapsed $p$ (i.e., $C(p, p)$) has the hereditary property: If $x$ (set) is in it, then so are the members of $x$, and – repeating this observation – so are the members of the members of $x$, and so on. □

**VI.2.38 Example (Continuation of Example VI.2.36).** We now examine whether the concrete $p$ of the previous example is a possible "universe" of sets and urelements, where we are content to live (mathematically speaking) and "do set theory" (i.e., it is the underlying *set* of some model of ZFC).[†] We discover that this *potential* "universe" has a disturbing property: Even though – *as inhabitants of p* – we "know" about certain two of its members, $x$ and $x'$, that[‡] $(\forall z)(z \in x \leftrightarrow z \in x')$, yet it happens that "really" $x \neq x'$. That is, *extensionality* fails in this universe.

Let us call a set $p$ *extensional* iff it satisfies (3) below (otherwise it is called *nonextensional*):

$$(\forall u \in p)(\forall v \in p)\Big(\neg U(u) \to \neg U(v) \to \\ (\forall z \in p)\big((z \in u \leftrightarrow z \in v) \to u = v\big)\Big) \tag{3}$$

It turns out that if $p$ is extensional to begin with, then by collapsing it, not only do we turn it into a transitive set, but also, the new set $C(p, p)$ is essentially the same as $p$; its elements are obtained by a judicious renaming of the elements of $p$, otherwise leaving the {}-structure of $p$ intact.

[†] By our belief that ZFC is consistent – cf. II.4.5 – set universes exist by the completeness theorem of Chapter I. However, this *p cannot* be one of them, for extensionality fails in it.

[‡] Caution: Since $p$ is (supposed to be) the "universe", "$(\forall z)$" here is short for "$(\forall z \in p)$".

More precisely, there is a 1-1 correspondence between $p$ and $C(p, p)$ ($x \mapsto C(p, x)$ does the "renaming") which preserves membership relationships (we get, technically, an isomorphism with respect to $\in$).

Let us prove this. If $p$ is extensional, then

$$\lambda x.C(p, x) : p \to C(p, p)$$

is a 1-1 correspondence such that, for all $x$, $y$ in $p$

$$x \in y \quad \text{iff} \quad C(p, x) \in C(p, y) \tag{4}$$

To this end, observe that $\lambda x.C(p, x) \restriction p$ is, trivially, total and that

$$\begin{aligned} \operatorname{ran}(\lambda x.C(p, x) \restriction p) &= \{C(p, y) : y \in p\} \\ &= C(p, p) \end{aligned}$$

so that $\lambda x.C(p, x) \restriction p$ is onto as well. Also observe that since

$$C(p, y) = \{C(p, u) : u \in y \cap p\}$$

we have

$$x \in p \wedge x \in y \to C(p, x) \in C(p, y)$$

which is half of (4). To conclude we need to show the 1-1-ness of $\lambda x.C(p, x) \restriction p$ as well as the if part of (4) above.

We show that

$$(\forall x)(\forall y)\mathscr{Q}(x, y) \tag{5}$$

where $\mathscr{Q}(x, y)$ stands for

$$\begin{aligned} &[C(p, x) = C(p, y) \to x = y] \wedge \\ &[C(p, x) \in C(p, y) \to x \in y] \wedge \\ &[C(p, y) \in C(p, x) \to y \in x] \end{aligned}$$

and *quantification is over* $p$.

We argue by contradiction, assuming instead the negation of (5):

$$(\exists x)(\exists y)\neg\mathscr{Q}(x, y) \tag{5$'$}$$

The argument is extremely close to that of the proof of trichotomy (V.1.20).

So, let $x_0$ be $\in$-minimal such that

$$(\exists y)\neg\mathscr{Q}(x_0, y) \tag{6}$$

and, similarly, $y_0$ be $\in$-minimal such that

$$\neg\mathscr{Q}(x_0, y_0) \tag{7}$$

We will contradict (7), which says that

$$\begin{aligned}&(C(p, x_0) = C(p, y_0) \wedge x_0 \neq y_0)\\ \vee\,&(C(p, x_0) \in C(p, y_0) \wedge x_0 \notin y_0)\\ \vee\,&(C(p, y_0) \in C(p, x_0) \wedge y_0 \notin x_0)\end{aligned}$$

*Case 1.* $C(p, x_0) = C(p, y_0) \wedge x_0 \neq y_0$ *(refutation of 1-1-ness).* If either $x_0$ or $y_0$ is an urelement, then $x_0 = y_0$, a contradiction. Indeed, say $x_0$ is an atom. Then $x_0 = C(p, x_0) = C(p, y_0)$, which forces $C(p, y_0)$ to be an urelement, inevitably $y_0$ (why?). So let both $x_0$ and $y_0$ be sets.

We will prove that $x_0 = y_0$ to obtain a contradiction. Since $p$ is extensional, this amounts to proving $z \in x_0 \rightarrow z \in y_0$ and $z \in y_0 \rightarrow z \in x_0$ for the arbitrary $z \in p$.

To this end, let $z \in x_0$, so (by (6)), $(\forall y)\mathscr{Q}(z, y)$ holds, in particular

$$\mathscr{Q}(z, y_0) \tag{8}$$

By the only-if part of (4), already proved, $z \in x_0$ yields $C(p, z) \in C(p, x_0) = C(p, y_0)$. Thus, by (8), $z \in y_0$.

One similarly proves $z \in y_0 \rightarrow z \in x_0$. However, it is instructive to include the full proof here, so that we can make a comment.

Let $z \in y_0$. By (7),

$$\mathscr{Q}(x_0, z) \tag{9}$$

By half of (4), $C(p, z) \in C(p, y_0) = C(p, x_0)$. By (9) $z \in x_0$.

Note that the inclusion of the seemingly redundant "$\wedge[C(p, y) \in C(p, x) \rightarrow y \in x]$" in the definition of $\mathscr{Q}(x, y)$ ensures the symmetry in the roles of $x$, $y$. In the absence of such symmetry, (9) would not help here.

*Case 2.* $C(p, x_0) \in C(p, y_0)$ *– hence* $y_0$ *is not an urelement – yet* $x_0 \notin y_0$. Thus

$$C(p, x_0) = C(p, z) \tag{10}$$

for some $z \in p \cap y_0$; hence (by (7)) $\mathscr{Q}(x_0, z)$; and (by (10)) $x_0 = z$, thus $x_0 \in y_0$, contradicting the assumption.

*Case 3.* $C(p, y_0) \in C(p, x_0)$, *yet* $y_0 \notin x_0$. This case leads to a contradiction, exactly like the previous one, establishing (5).

Thus, if $\mathscr{A} = (A, U, \in)$ is a *countable* model of ZFC,[†] then $(C(A, A), U, \in)$ is an isomorphic ($=$, $U$ and $\in$ are "preserved") *transitive model.* A so-called CTM (countable transitive model). Cf. I.7.12. □ ☡☡

[†] Such models exist by the Löwenheim-Skolem theorem of Chapter I, since the language of ZFC is countable (granting that ZFC is consistent).

**VI.2.39 Example (Example VI.2.36 Concluded).** Let $p = \{\#, !, ?, \{\#, @, ?\}, \{\#, !\}\}$. Set $x = \{\#, @, ?\}$ and $x' = \{\#, !\}$. This $p$ is extensional for $p \cap x \neq p \cap x'$. One easily computes

$$C(p, x) = \{\#, ?\}$$

and

$$C(p, x') = \{\#, !\}$$

Thus the collapse of $p$, $C(p, p)$, is $\{\#, !, ?, \{\#, ?\}, \{\#, !\}\}$. □

We conclude this section with an extension of the previous recursive definition schemata – which define *one* function – to the case where many functions are defined at once by *simultaneous recursion*. This tool – familiar to the worker in computability, where it goes back (at least) to Hilbert and Bernays (1968) – will be handy in our last chapter, on *forcing*. There are many variations that are left to the reader's imagination. We just give two of the many possible schemata here and also restrict the number of functions that are simultaneously defined to just two (without loss of generality, as the reader will readily attest).

**VI.2.40 Corollary (Simultaneous Recursion with Respect to an Arbitrary Relation with IC).** *Let $\mathbb{P} : \mathbb{A} \to \mathbb{A}$ be a left-narrow relation – not necessarily an order – with IC, and $\mathbb{G}_1$ and $\mathbb{G}_2$ (not necessarily total) functions $\mathbb{A} \times \mathbb{U}_M^2 \to \mathbb{X}$, for some class $\mathbb{X}$. Then there exist unique functions $\mathbb{F}_1$ and $\mathbb{F}_2$, from $\mathbb{A}$ to $\mathbb{X}$, satisfying*

$$(\forall a \in \mathbb{A})\mathbb{F}_1(a) \simeq \mathbb{G}_1\big(a, \{\langle x, \mathbb{F}_1(x)\rangle : x \,\mathbb{P}\, a\}, \{\langle x, \mathbb{F}_2(x)\rangle : x \,\mathbb{P}\, a\}\big) \qquad (1)$$

*and*

$$(\forall a \in \mathbb{A})\mathbb{F}_2(a) \simeq \mathbb{G}_2\big(a, \{\langle x, \mathbb{F}_1(x)\rangle : x \,\mathbb{P}\, a\}, \{\langle x, \mathbb{F}_2(x)\rangle : x \,\mathbb{P}\, a\}\big) \qquad (2)$$

*Proof.* We define functions $p_1$ and $p_2$ by

$$p_1(f) = \begin{cases} \uparrow & \text{if } f \text{ is } \textit{not} \text{ a class of } \langle x, \langle y, z\rangle\rangle\text{-type entries} \\ \{\langle \pi(z), \pi(\delta(z))\rangle : z \in f\} & \text{otherwise} \end{cases}$$

and

$$p_2(f) = \begin{cases} \uparrow & \text{if } f \text{ is } \textit{not} \text{ a class of } \langle x, \langle y, z\rangle\rangle\text{-type entries} \\ \{\langle \pi(z), \delta(\delta(z))\rangle : z \in f\} & \text{otherwise} \end{cases}$$

and set

$$\mathbb{G} = \lambda xf.\big\langle \mathbb{G}_1\big(x, p_1(f), p_2(f)\big), \mathbb{G}_2\big(x, p_1(f), p_2(f)\big)\big\rangle$$

By VI.2.27 there is a unique $\mathbb{F} : \mathbb{A} \to \mathbb{X}$ such that

$$(\forall a \in \mathbb{A})\mathbb{F}(a) \simeq \mathbb{G}\big(a, \{\langle x, \mathbb{F}(x)\rangle : x \, \mathbb{P} \, a\}\big)$$

It is trivial to check (induction) that $\mathbb{F}$ is a class of $\langle x, \langle y, z\rangle\rangle$-type entries (equivalently, $\mathbb{F}(a) \downarrow$ implies that $\mathbb{F}(a)$ is a pair). Taking $\mathbb{F}_1 = \pi \circ \mathbb{F}$ and $\mathbb{F}_2 = \delta \circ \mathbb{F}$, we have satisfied (1) and (2) respectively. □

**VI.2.41 Corollary (Simultaneous Recursion with a Total $\mathbb{G}$).** *Let $\mathbb{P} : \mathbb{A} \to \mathbb{A}$ be a left-narrow relation – not necessarily an order – with IC, and $\mathbb{G}_1$ and $\mathbb{G}_2$ total functions $\mathbb{A} \times \mathbb{U}_M^2 \to \mathbb{X}$ for some class $\mathbb{X}$. Then there exist unique total functions $\mathbb{F}_1$ and $\mathbb{F}_2$ from $\mathbb{A}$ to $\mathbb{X}$ satisfying*

$$(\forall a \in \mathbb{A})\mathbb{F}_1(a) = \mathbb{G}_1(a, \mathbb{F}_1 \restriction \mathbb{P}\langle a\rangle, \mathbb{F}_2 \restriction \mathbb{P}\langle a\rangle)$$

*and*

$$(\forall a \in \mathbb{A})\mathbb{F}_2(a) = \mathbb{G}_2(a, \mathbb{F}_1 \restriction \mathbb{P}\langle a\rangle, \mathbb{F}_2 \restriction \mathbb{P}\langle a\rangle)$$

## VI.3. Comparing Orders

**VI.3.1 Example (Informal).** Consider $R \subseteq A \times A$, where $A = \{1, 2, 3\}$ and the relation $R = \{\langle 1, 2\rangle, \langle 2, 3\rangle, \langle 1, 3\rangle\}$. Also consider $S \subseteq B \times B$, where $B = \{a, b, c\}$ and $S = \{\langle a, b\rangle, \langle b, c\rangle, \langle a, c\rangle\}$.

$(A, R)$ and $(B, S)$ are PO sets (indeed, WO sets). What is interesting here is that once we are given the first PO set, the second one does not offer any new information as far as partial order or, indeed, well-ordering is concerned. This observation holds true if "first" and "second" are interchanged.

This is because $(B, S)$ is obtained from $(A, R)$ by a systematic renaming of objects ($1 \mapsto a, 2 \mapsto b, 3 \mapsto c$) which *preserves order*. That is, $f = \{\langle 1, a\rangle, \langle 2, b\rangle, \langle 3, c\rangle\}$ is a 1-1 correspondence $A \to B$ such that $x \, R \, y$ iff $f(x) S f(y)$.

Since such a correspondence exhibits the fact that $(A, R)$ and $(B, S)$ have the same "shape", or "form" (loosely translated into Greek, the same "$\mu o \rho \phi \acute{\eta}$", or "morphē" in transliteration), it has been given the standard name *isomorphism*.[†]

[†] Strictly speaking, *order isomorphism* in this case, since the concept of isomorphism extends to other mathematical structures as well. The prefix "iso" in the term comes from the Greek word *ίσο*, which means "equal" or "identical".

If we have complete knowledge of $(A, R)$ (respectively $(B, S)$), it is as good as having complete knowledge of $(B, S)$ (respectively $(A, R)$). It suffices to study any convenient *one* out of many mutually order-isomorphic PO sets (or LO sets or WO sets). □

**VI.3.2 Example (Informal).** $(\mathbb{N}, <)$ and $(\{-2, -1\} \cup \mathbb{N}, <)$ are order-isomorphic PO sets, where the "$<$" is the standard order (they are also order-isomorphic WO sets).

Indeed, if we let $f : \mathbb{N} \to \{-2, -1\} \cup \mathbb{N}$ be $\lambda x.x - 2$, then clearly $f$ is a 1-1 correspondence and $i < j$ iff $f(i) < f(j)$ for all $i, j$ in $\mathbb{N}$. □

Now some definitions and some useful results.

**VI.3.3 Informal Definition.** Let $(\mathbb{A}, \mathbb{S})$ and $(\mathbb{B}, \mathbb{T})$ be two PO classes. A 1-1 correspondence $f : \mathbb{A} \to \mathbb{B}$ is an *order-isomorphism* just in case

$$x \, \mathbb{S} \, y \text{ iff } f(x) \, \mathbb{T} \, f(y) \qquad \text{for all } \{x, y\} \subseteq \mathbb{A}.$$

$(\mathbb{A}, \mathbb{S})$ and $(\mathbb{B}, \mathbb{T})$ are called *order-isomorphic*. We write $(\mathbb{A}, \mathbb{S}) \cong (\mathbb{B}, \mathbb{T})$. □

We will drop the qualification "order-" from "order-isomorphic" as long as the context ascertains that there is no other type of isomorphism in consideration.

We often abuse language (and notation) in those cases where the orders $\mathbb{S}$ (on $\mathbb{A}$) and $\mathbb{T}$ (on $\mathbb{B}$) are clearly understood from the context. We then say simply that $\mathbb{A}$ and $\mathbb{B}$ are isomorphic and write $\mathbb{A} \cong \mathbb{B}$. As usual, the negation of $\cong$ is written $\ncong$.

A notion related to isomorphism is that of an *order-preserving function*.

**VI.3.4 Informal Definition.** Let $(\mathbb{A}, \mathbb{S})$ and $(\mathbb{B}, \mathbb{T})$ be two PO classes, and $f : \mathbb{A} \to \mathbb{B}$ be total. If, on the assumption that $x \in \mathbb{A} \wedge y \in \mathbb{A}$, the implication $x \, \mathbb{S} \, y \to f(x) \, \mathbb{T} \, f(y)$, holds, then $f$ is called *order-preserving*. □

**VI.3.5 Remark.** *Operationally*, "holds" above can only be certified by a ZFC proof (when such proof is possible). Correspondingly, the *act of assuming*, in the course of a proof, that a certain total $f : \mathbb{A} \to \mathbb{B}$ is order-preserving between the PO classes $(\mathbb{A}, \mathbb{S})$ and $(\mathbb{B}, \mathbb{T})$ is tantamount to *adding* the axiom

$$x \in \mathbb{A} \wedge y \in \mathbb{A} \to x \, \mathbb{S} \, y \to f(x) \, \mathbb{T} \, f(y)$$

If we use the more natural notation $<_1$ and $<_2$ for $\mathbb{S}$ and $\mathbb{T}$ respectively, then the above definition says that $x <_1 y \to f(x) <_2 f(y)$ is the condition for a total $f$ to be order-preserving. □

**VI.3.6 Example (Informal).** Let $A = \{a, b, c, d\}$ be equipped with the order $<_1$ so that (just) $a <_1 b$. Let $B = \{1, 2\}$ be equipped with the order $<_2$ so that (just) $1 <_2 2$.

Define $f = \{\langle a, 1\rangle, \langle b, 2\rangle, \langle c, 1\rangle, \langle d, 1\rangle\}$. Clearly, $f : A \to B$ is order-preserving, since the statement

$$(\forall x \in A)(\forall y \in A)(x <_1 y \to f(x) <_1 f(y))$$

is true. However, note that $f$ is not 1-1; hence it is not an isomorphism. □

**VI.3.7 Example (Informal).** Let $A = \{a, b, c, d\}$ be equipped with the order $<_1$ so that (just) $a <_1 b$. Let $B = \{1, 2, 3, 4\}$ be equipped with the order $<_2$ so that $1 <_2 2 <_2 3 <_2 4$ (employing "$<_2$" conjunctionally). Define $g$ as $\{\langle a, 1\rangle, \langle b, 2\rangle, \langle c, 3\rangle, \langle d, 4\rangle\}$. Then $g$ is order-preserving. It is also a 1-1 correspondence, but *not* an isomorphism, since $g(c) <_2 g(d)$ but $c \not<_1 d$. In fact, $c$ and $d$ are non-comparable under $<_1$. □

**VI.3.8 Proposition.** *Let* $(\mathbb{A}, <_1)$ *be a LO class,* $(\mathbb{B}, <_2)$ *be a PO class, and* $f : \mathbb{A} \to \mathbb{B}$ *be order-preserving (see VI.3.5 for the interpretation of these assumptions). Then*

(a) $f$ *is* 1–1*, and*
(b) $f$ *is an isomorphism between* $(\mathbb{A}, <_1)$ *and* $(\mathrm{ran}(f), <_2)$.

*Proof.* (a): Let $x \neq y$ in $\mathbb{A}$. As $<_1$ is a linear order, we have $x <_1 y$ or $y <_1 x$; let us examine only the latter case. Then $f(y) <_2 f(x)$; hence $f(x) \neq f(y)$, since the orders are irreflexive.

(b): Let $f(x) <_2 f(y)$ in $\mathrm{ran}(f)$. Since this implies $f(x) \neq f(y)$, we must have $x \neq y$ by single-valuedness of $f$. Thus we will have $x <_1 y$ or $y <_1 x$.

Let the latter be the case. Then also $f(y) <_2 f(x)$; hence by the assumption and transitivity of $<_2$, $f(x) <_2 f(x)$ – a contradiction.

We conclude that $x <_1 y$ is the only possible case. Therefore we have established that $f(x) <_2 f(y) \to x <_1 y$, which, along with $f$ being order-preserving, establishes $f$ as an isomorphism of LO classes. □

**VI.3.9 Remark.** A function such as $f$ is called an *embedding*. It embeds $(\mathbb{A}, <_1)$ into $(\mathbb{B}, <_2)$ in the sense that it shows the former to be an *isomorphic copy* of a *subclass* of $\mathbb{B}$ (here ran$(f)$), where, of course, this subclass is equipped with the same order as $\mathbb{B}$, namely $<_2$.

If ran$(f) = \mathbb{B}$, then the embedding is an isomorphism. □

**VI.3.10 Corollary.** *Let* $(\mathbb{A}, <_1)$ *be a LO class,* $\mathbb{B}$ *a class, and* $f : \mathbb{A} \to \mathbb{B}$ *a* 1-1 *correspondence. Define* $x <_2 y$ *on* $\mathbb{B}$ *by* $f^{-1}(x) <_1 f^{-1}(y)$.

*Then* $(\mathbb{B}, <_2)$ *is a LO class that is isomorphic to* $(\mathbb{A}, <_1)$.

**VI.3.11 Remark.** We say that the order $<_2$ on $\mathbb{B}$ is *induced by* $f$ (and $<_1$). □

**VI.3.12 Corollary.** *If* $<_1$ *in* VI.3.10 *is a well-ordering, then* $(\mathbb{B}, <_2)$ *is a WO class isomorphic to* $(\mathbb{A}, <_1)$.

*Proof.* Let $\emptyset \neq \mathbb{X} \subseteq \mathbb{B}$, and let $a = \min(f^{-1}[\mathbb{X}])$. Now, $x \in \mathbb{X}$ implies $f^{-1}(x) \in f^{-1}[\mathbb{X}]$; hence $a \leq_1 f^{-1}(x)$; thus $f(a) \leq_2 x$. That is, $f(a) = \min(\mathbb{X})$. □

**VI.3.13 Proposition.** *Let* $(\mathbb{A}, <)$ *be a PO class with MC, and* $f : \mathbb{A} \to \mathbb{A}$ *be order-preserving. Then there is no* $x \in \mathbb{A}$ *such that* $f(x) < x$.

*Proof.* Assume the contrary, and let $m$ be minimal in $\mathbb{B} = \{x \in \mathbb{A} : f(x) < x\}$. Thus,

$$f(m) < m \tag{1}$$

Since $f$ is order-preserving, (1) yields

$$f(f(m)) < f(m) \tag{2}$$

By (2), $f(m) \in \mathbb{B}$, which by (1) contradicts the minimality of $m$. □

**VI.3.14 Remark.** Another way to see the reason for the above is to observe that if for any $a \in \mathbb{A}$

$$f(a) < a$$

holds, then

$$\cdots < f(f(f(a))) < f(f(a)) < f(a) < a$$

is an infinite descending chain, contradicting VI.2.11. □

**VI.3.15 Corollary.** *If* $(\mathbb{A}, <)$ *is a WO class and* $f : \mathbb{A} \to \mathbb{A}$ *is order-preserving, then* $(\forall x \in \mathbb{A})x \leq f(x)$.

The following two corollaries use the notion of segment in their formulation (see VI.2.24).

**VI.3.16 Corollary.** *There is no isomorphism between a WO class and one of its segments.*

*Proof.* Say $(\mathbb{A}, <)$ is a WO class and $f : \mathbb{A} \to < \langle a \rangle$ is an isomorphism, where $a \in \mathbb{A}$. Then $f(a) \in < \langle a \rangle$, that is, $f(a) < a$, a contradiction. □

**VI.3.17 Corollary.** *Given a WO class* $(\mathbb{A}, <)$. *If* $a \in \mathbb{A}$ *and* $\leq \langle a \rangle \subset \mathbb{A}$, *then there is no isomorphism* $f : \mathbb{A} \to \leq \langle a \rangle$.

*Proof.* Let $b \in \mathbb{A} - \leq \langle a \rangle$. Thus $a < b$; hence (conjunctionally) $f(b) \leq a < b$, contradicting VI.3.13. □

**VI.3.18 Corollary.** *If* $(\mathbb{A}, <)$ *is a WO class, and* $f : \mathbb{A} \to \mathbb{A}$ *is an isomorphism, then* $f = \Delta_{\mathbb{A}}$.

*Proof.* Let instead $f(a) \neq a$ for some $a \in \mathbb{A}$. If $a < f(a)$, then applying the order-preserving $f^{-1}$ to both sides, we get $f^{-1}(a) < a$, contradicting VI.3.13. For the same reason, the hypothesis $f(a) < a$ is rejected outright. □

**VI.3.19 Corollary.** *If* $(\mathbb{A}, <_1)$ *and* $(\mathbb{B}, <_2)$ *are isomorphic WO classes, then there is exactly one isomorphism* $f : \mathbb{A} \to \mathbb{B}$.

*Proof.* Let $f : \mathbb{A} \to \mathbb{B}$ and $g : \mathbb{A} \to \mathbb{B}$ be isomorphisms. It is trivially verifiable that $g^{-1} \circ f : \mathbb{A} \to \mathbb{A}$ is an isomorphism.

By VI.3.18, $g^{-1} \circ f = \Delta_{\mathbb{A}}$; hence $f = g$, since both functions are 1-1 correspondences. □

The next result shows, on one hand, that if two WO classes are not isomorphic, then one properly contains (an isomorphic copy of) the other, i.e., the "smaller" of the two is embeddable in the "larger". On the other hand, it shows that every WO class has the structure of (i.e., is isomorphic to) a segment.

**VI.3.20 Theorem.** *Let* $(\mathbb{A}, <_1)$ *and* $(\mathbb{B}, <_2)$ *be any WO classes and* $<_1$ *be left-narrow. Then exactly one of the following cases obtains:*

(a) *The two WO classes are isomorphic,*
(b) $(\mathbb{A}, <_1)$ *is isomorphic to a segment of* $(\mathbb{B}, <_2)$,
(c) $(\mathbb{B}, <_2)$ *is isomorphic to a segment of* $(\mathbb{A}, <_1)$.

*Proof.* By VI.3.16 no two of the above three cases are possible at once. It remains to prove the disjunction of (a)–(c). Intuitively, we start off by pairing $\min(\mathbb{A})$ with $\min(\mathbb{B})$. Then we pair the "next larger" element of $\mathbb{A}$ with that of $\mathbb{B}$. We continue in this way until either we run out of elements from $\mathbb{A}$ and $\mathbb{B}$ simultaneously, or deplete $\mathbb{A}$ first, or deplete $\mathbb{B}$ first (these cases correspond to the ones enumerated (a)–(c) in the theorem).

Formally now, if any of $\mathbb{A}$ or $\mathbb{B}$ is $\emptyset$, then the result is trivial. So let $\mathbb{A} \neq \emptyset \neq \mathbb{B}$, and apply the pure recursion (VI.2.31) to define the function $\mathbb{F} : \mathbb{A} \to \mathbb{B}$ by

$$(\forall x \in \mathbb{A})\mathbb{F}(x) \simeq \min \left\{ y : y \in \mathbb{B} - \mathrm{ran}(\mathbb{F} \restriction <_1 \langle x \rangle) \right\} \tag{1}$$

Next, we establish that $\mathbb{F} : \mathrm{dom}(\mathbb{F}) \to \mathrm{ran}(\mathbb{F})$ is an isomorphism. By VI.3.8, it suffices to show that it is order-preserving on its domain. To see this we show that

$$(\forall y)(y \in \mathrm{ran}(\mathbb{F} \restriction <_1 \langle x \rangle) \to y <_2 \mathbb{F}(x)) \tag{2}$$

Assume instead (recall that $<_2$ is total)

$$(\exists y)(y \in \mathrm{ran}(\mathbb{F} \restriction <_1 \langle x \rangle) \wedge \mathbb{F}(x) \leq_2 y) \tag{2$'$}$$

Because of (2$'$) we may add the assumption

$$c \in \mathrm{ran}(\mathbb{F} \restriction <_1 \langle x \rangle) \wedge \mathbb{F}(x) \leq_2 c \tag{3}$$

where $c$ is a new constant. Let $b \in <_1 \langle x \rangle$ (another auxiliary constant) such that $\mathbb{F}(b) = c$. By (1),

$$z \in \mathbb{B} - \mathrm{ran}(\mathbb{F} \restriction <_1 \langle b \rangle) \to \mathbb{F}(b) \leq_2 z \tag{4}$$

By (1) again, $\mathbb{F}(x) \notin \mathrm{ran}(\mathbb{F} \restriction <_1 \langle x \rangle)$ (in particular, $y <_1 x \to \mathbb{F}(y) \neq \mathbb{F}(x)$, i.e., $\mathbb{F}$ is 1-1); hence $\mathbb{F}(x) \notin \mathrm{ran}(\mathbb{F} \restriction <_1 \langle b \rangle)$ by $<_1 \langle b \rangle \subset <_1 \langle x \rangle$.

Thus

$$\mathbb{F}(b) <_2 \mathbb{F}(x)$$

by (1), (4) and 1-1-ness of $\mathbb{F}$ (the last property sharpens "$\leq_2$" to "$<_2$"). This contradicts (3) since $c = \mathbb{F}(b)$. We have established (2).

By VI.2.31 we have one of

$$\mathrm{dom}(\mathbb{F}) = \mathbb{A} \tag{5}$$

or

$$\mathrm{dom}(\mathbb{F}) = <_1 \langle a \rangle \qquad \text{for some } a \in \mathbb{A} \tag{6}$$

Before proceeding we show that

$$x \in \operatorname{ran}(\mathbb{F}) \rightarrow <_2 \langle x \rangle \subseteq \operatorname{ran}(\mathbb{F}) \tag{7}$$

This is trivial if $\operatorname{ran}(\mathbb{F}) = \mathbb{B}$. Let then $x \in \operatorname{ran}(\mathbb{F})$, and take

$$c \in \mathbb{B} - \operatorname{ran}(\mathbb{F}) \tag{8}$$

(a new auxiliary constant) such that

$$c <_2 x \tag{9}$$

Let $x = \mathbb{F}(y)$. By (1) and (8)

$$\mathbb{F}(y) \leq_2 c$$

contradicting (9). This settles (7). We immediately conclude that

If $\operatorname{ran}(\mathbb{F}) \neq \mathbb{B}$, then $\operatorname{ran}(\mathbb{F}) = <_2 \langle b \rangle$, where $b = \min\{y : y \in \mathbb{B} - \operatorname{ran}(\mathbb{F})\}$.

Suppose now that (5) is the case. If also $\operatorname{ran}(\mathbb{F}) = \mathbb{B}$, then we are done in this case. If on the other hand $\operatorname{ran}(\mathbb{F}) \neq \mathbb{B}$, then $\operatorname{ran}(\mathbb{F})$ is a segment by the above, so we are done in this case.

Suppose finally that (6) is the case. Thus $\operatorname{ran}(\mathbb{F})$ is either all of $\mathbb{B}$ or a segment, $<_2 \langle b \rangle$.

We will retire the proof if we show this latter subcase to be untenable: Indeed, the function $\mathbb{F} \cup \{\langle a, b \rangle\}$ properly extends $\mathbb{F}$, still satisfying (1) –

**Pause.** Do you believe this?

contradicting uniqueness of $\mathbb{F}$ (VI.2.31). □

**VI.3.21 Remark.** The above theorem can form the basis for the comparability of ordinals of the next section. Alternatively, one can prove the comparability of ordinals directly and derive VI.3.20 (for WO *sets*) as a corollary (VI.3.23 below). We will return to this remark in the next section. □

**VI.3.22 Exercise.**

(i) If $<_2$ is known *not* to be left-narrow (the statement of the theorem allows either possibility), then how are cases (a)–(c) affected?

(ii) Suppose that $<_2$ *is* left-narrow as well, and $\mathbb{A}$ and $\mathbb{B}$ are proper classes. What now? □

**VI.3.23 Corollary.** *Let* $(\mathbb{A}, <_1)$ *and* $(\mathbb{B}, <_2)$ *be any WO* sets. *Then exactly one of the following cases obtains:*

(a) *The two WO sets are isomorphic,*
(b) $(\mathbb{A}, <_1)$ *is isomorphic to a segment of* $(\mathbb{B}, <_2)$*,*
(c) $(\mathbb{B}, <_2)$ *is isomorphic to a segment of* $(\mathbb{A}, <_1)$.

## VI.4. Ordinals

Let $(A, <)$ be a WO *set*, where $A \neq \emptyset$. Let $a_0 = \min(A)$. If $A - \{a_0\} \neq \emptyset$, then let $a_1 = \min(A - \{a_0\})$. In general, if $A - \{a_0, a_1, \ldots, a_n\} \neq \emptyset$, then define $a_{n+1}$ to be $\min(A - \{a_0, a_1, \ldots, a_n\})$.

Possibly, for some smallest $n \in \mathbb{N}$, $A - \{a_0, a_1, \ldots, a_n\} = \emptyset$, and thus $A = \{a_0, a_1, \ldots, a_n\}$, so that $a_0 < a_1 < \cdots < a_n$.

Another possibility, when $A$ is (intuitively[†]) infinite is, that we will *exactly* need *all* the natural numbers in $\mathbb{N}$ in order to name the positions of the elements of $A$ in their (ascending) $<$-order; that is, $A = \{a_0, a_1, \ldots\}$ and $a_0 < a_1 < \cdots$.

Is it possible that a WO set is so "long" that we will run out of position *names* (from $\mathbb{N}$) before we run out of *positions* in $A$? The answer (affirmative) is straightforward:

**VI.4.1 Example (Informal).** Adjoin to $\mathbb{N}$ – equipped with the "natural order" $<= \{\langle i+1, i\rangle : i \in \mathbb{N}\}$ – a new object. For example, adjoin the new object $\mathbb{N}$ ("new" in the sense that $\mathbb{N} \notin \mathbb{N}$) to form $A = \mathbb{N} \cup \{\mathbb{N}\}$.

Next, extend $<$ to $<_A$ on $A$ by $<_A = < \cup \{\langle \mathbb{N}, i\rangle : i \in \mathbb{N}\}$. That is, $i <_A \mathbb{N}$ for all $i \in \mathbb{N}$.

The requirement that the object $\mathbb{N}$ have a position immediately *after all* the $i$'s in $\mathbb{N}$ forces us to run out of position names (supplied from $\mathbb{N}$) when we are naming the positions of the elements of the WO set $A$. Object $\mathbb{N}$ is the first in $A$ that has no position name, if the name supply is just $\mathbb{N}$.

Mathematicians use the name $\omega$ (the same one used for the set of formal natural numbers) to name the position of $\mathbb{N}$ in $A$ (that is, the first position after positions $0, 1, 2, \ldots$). Thus $A$ is the "ordered sequence" $a_0 <_A a_1 <_A a_2 <_A \cdots <_A a_\omega$.

We can carry this further. We can imagine a WO set $(B, <_B)$ that is so long that it requires yet another position name after $\omega$. We call this new position $\omega + 1$, so that $B$ is the ordered sequence $b_0 <_B b_1 <_B b_2 <_B <_B \cdots <_B b_\omega <_B b_{\omega+1}$.

[†] We are going to formalize the notions "finite" and "infinite" in Chapter VII.

Similarly, for still longer WO sets one invents position names $\omega + 2$, $\omega + 3$, etc.

What would be the name for the position immediately after *all* the ones named $\omega + i$ ($i \in \mathbb{N}$)? Mathematicians have invented the name "$\omega \cdot 2$". □

These position names of WO set elements are the so-called *ordinals* (also called *ordinal numbers*). They provide (among other things) an extension of the position-naming apparatus that $\mathbb{N}$ is.

In order to eventually come up with a well-motivated formal definition of ordinals, let us speculate a bit further on their nature. Extrapolating from the discussion of Example VI.4.1, let us imagine a sequence of position names $0, 1, \ldots, \omega, \omega + 1, \ldots, \omega \cdot 2, \omega \cdot 2 + 1, \ldots, \omega \cdot 3, \omega \cdot 3 + 1, \ldots$ of sufficient length so that the elements of *any* WO set $(A, <)$ can fit, in ascending order (with respect to the WO set's own "$<$") contiguously from left to right in named position slots (starting with the 0th position slot).

Once we have so fitted $(A, <)$, let the ordinal $\alpha$ be the *first unused position name*. This $\alpha$ characterizes the "form" or "type" of the WO set $(A, <)$, in the sense that if $(B, <_1)$ is another WO set such that $(A, <) \cong (B, <_1)$, then the elements of $B$, in view of

$$\begin{aligned} A &: a_0 < a_1 < \cdots < a_\gamma \ldots \\ B &: b_0 < b_1 < \cdots < b_\gamma \ldots \end{aligned}$$

will occupy exactly the same positions as the $A$-elements, and thus, once again, $\alpha$ will be the first unused position name.

Hence, a formal definition of ordinals must ensure that they are *objects* of set theory associated with WO sets in such a way that the same ordinal corresponds to each WO set in a class of pairwise isomorphic WO sets. That is, one looks for a function $\| \ldots \|$ , defined on all WO sets, such that

$$\|(A, <_1)\| = \|(B, <_2)\| \quad \text{iff} \quad \text{(as WO sets)} \quad (A, <_1) \cong (B, <_2)$$

The range of $\| \ldots \|$ will be the class of all ordinals – which turns out to be a proper class.

The above observations led to Cantor's original definition:

**VI.4.2 Tentative Definition.** (See Wilder (1963, p. 111).) The *ordinal* or *ordinal number* of a WO set $(A, <)$ is the class of all WO sets $(B, <_1)$ such that $(A, <) \cong (B, <_1)$. □

The "permanent" definition will be given in VI.4.16.

**VI.4.3 Remark.** The reader can readily verify that $\cong$ is an equivalence relation on the class of all WO sets. Thus, the above definition adopts $(A, <) \mapsto \big[(A, <)\big]_{\cong}$ (recall the notation introduced in V.4.3) as the function $\| \ldots \|$.

It turns out that the equivalence classes $[\ldots]_{\cong}$ are too big to be sets (Exercise VI.7), so that they are inappropriate as formal objects of the theory. □

Therefore we try next

**VI.4.4 Tentative Definition.** (See Kamke (1950, p. 57).) The *ordinal* or *ordinal number* of a WO set $(A, <)$ is an arbitrary representative out of $\big[(A, <)\big]_{\cong}$. □

The new definition gets around the difficulty mentioned in VI.4.3. However, it creates a great sense of uncertainty with the indefinite ("an arbitrary representative") manner in which an ordinal is "defined". To conclude this discussion that peeks into the history of the development of ordinals (mostly by Cantor), let us try and fix the latest tentative definition (VI.4.4) so that we can appreciate that the old-fashioned way of introducing ordinals could be made to work. We will fix the definition and follow up some of its early consequences. Once this is done, we will have on hand enough motivational ideas to start from scratch with von Neumann's modern definition. The reader will benefit from knowing both points of view.

**Warning.** All these tentative definitions are *informal* and deal with metamathematical concepts.

**VI.4.5 Tentative Definition.** The *ordinal* or *ordinal number* of a WO set $(A, <)$, in symbols $\|(A, <)\|$, is that element of $\big[(A, <)\big]_{\cong}$ picked up by the *principle*[†] of global (strong) choice. "On" denotes the class of all ordinals. □

We are *not* committing ourselves above to an assumption that we have strong or global choice, an assumption that would entail (indeed, would be equivalent to – see the informal discussion in Section IV.2) the well-orderability of $\mathbb{U}_M$.

The reader is strongly reminded that, until the definitive definition of ordinals in VI.4.16 below, all that these tentative attempts towards a definition do is to outline briefly the history that led to the definitive definition. For this reason, any auxiliary assumptions introduced to make these tentative definitions tenable will be discarded as soon as we reach VI.4.16.

[†] We avoid the term "axiom". The reason is explained in the commentary following the definition.

We have the following trivial consequence of this definition:

**VI.4.6 Proposition (Informal).** $\|(A, <_1)\| = \|(B, <_2)\|$ *iff* $(A, <_1) \cong (B, <_2)$ *for any two WO sets.*

**VI.4.7 Remark.** All along, when we wrote $(A, R)$ for a set $A$ equipped with a relation $R \subseteq A \times A$, the symbol $(\ldots, \ldots)$ was used informally, simply to remind us of the two ingredients of the situation, namely $A$ and $R$ (see also the footnote to VI.1.11).

In instances such as Tentative Definitions VI.4.2–VI.4.5, for example in uses such as $\|(A, R)\|$, one would expect to use the formal $\langle A, R\rangle$ instead, so that the "pair" of $A$ and $R$ is an object of the theory (a set). However, we will continue using round brackets to denote PO sets, as we have previously agreed to do.

Ordinals will be denoted by lowercase Greek letters, in general. Notation for *specific* ordinals may differ (see the following example). □

**VI.4.8 Example (Informal).** What is $\|(\{0, 1\}, <)\|$, where $<$ is the standard order ($\in$) on $\omega$? According to VI.4.5, it is whichever WO set of exactly two elements (say, $(\{a, b\}, \{\langle b, a\rangle\})$ for some $a \neq b$) strong AC will pick out of the class $\big[(\{0, 1\}, <)\big]_{\cong}$. We naturally use a standard name, the symbol "2", to denote the ordinal of a WO set of two elements. This is summed up as

$$\|(\{a, b\}, \{\langle b, a\rangle\})\| = \|(2, <)\| = 2$$

since $2 = \{0, 1\}$.

Similarly, the symbol "$n$" (in $\omega$) will denote the ordinal $\|(n, <)\|$, where again, $<=\in$. Finally, we have already remarked that $\omega$ will be the short name for the ordinal $\|(\omega, \in)\|$. □

Next, we consider the ordering of ordinals.

**VI.4.9 Tentative Definition.** An order, $<$, is defined on On as follows: Let $\alpha$ and $\beta$ be two ordinals. Then $\alpha < \beta$ iff $\alpha$ is isomorphic to a segment of $\beta$. □

**VI.4.10 Remark (Informal).** Recall that $\alpha = (A, <_1)$ and $\beta = (B, <_2)$ for some appropriate $A$, $B$, $<_1$, $<_2$. Now, intuitively, $(A, <_1)$ can be embedded into $(B, <_2)$ as a segment iff the sequence

$$B : \ b_0 <_2 b_1 <_2 \cdots$$

is longer than the sequence

$$A:\ a_0 <_1 a_1 <_1 \cdots$$

and hence, iff the position *immediately to the right of the $A$-sequence is to the* left *of the position immediately to the right of the $B$-sequence.* The italicized text says, intuitively, that $\alpha < \beta$; therefore the above definition is consistent with our view that the ordinal of a WO set is the *position name* of the first position to the right of the set. □

**VI.4.11 Proposition (Informal).** *If $\alpha$ and $\beta$ are ordinals, then exactly one of $\alpha < \beta$, $\alpha = \beta$, $\beta < \alpha$ holds.*

*Proof.* Let $\alpha = (A, <_1)$ and $\beta = (B, <_2)$. By VI.3.23, exactly one of the following holds:

(a) $(A, <_1) \cong (B, <_2)$,
(b) $(A, <_1)$ is isomorphic to a segment of $(B, <_2)$,
(c) $(B, <_2)$ is isomorphic to a segment of $(A, <_1)$.

(b) and (c) say $\alpha < \beta$ and $\beta < \alpha$, respectively, by VI.4.9.

By (a), both $(A, <_1)$ and $(B, <_2)$ are in the same equivalence class. Since strong choice picks "deterministically" a unique representative from each equivalence class, and each of $(A, <_1)$ and $(B, <_2)$ is a representative, it follows that $(A, <_1) = (B, <_2)$, i.e., $\alpha = \beta$. □

**VI.4.12 Proposition (Informal).** On *is well-ordered by "$<$" of VI.4.9.*

*Proof.* By VI.4.11, $<$ is total. By VI.3.16, $<$ is irreflexive. The reader can verify that it is also transitive (Exercise VI.8). Therefore, $<$ is a linear order.

Let next $\emptyset \neq A \subseteq \mathrm{On}$ ($A$ need not be a set). Let $\alpha \in A$. If $\alpha = \min(A)$,[†] then we are done; otherwise $X = \{\beta \in A : \beta < \alpha\}$ is nonempty. Let $\alpha = (Y, <_1)$.

Next, if $\beta = (Z, <_2) \in X$, then (by VI.4.9) there is a unique

**Pause.** Why "unique"?

$y_\beta \in Y$ such that $\beta \cong (<_1 \langle y_\beta \rangle, <_1)$. By collection, $X$ is a set.

We show that there is a minimum $\beta$ in $X$. If not, then (VI.2.13) there is an infinite descending $<$-chain in $X$:

$$\cdots < \beta_3 < \beta_2 < \beta_1 \tag{1}$$

[†] The term "minimum" and "minimal" are interchangeable, since $<$ is total (VI.1.19).

This induces the infinite descending $<_1$-chain in $Y$:

$$\cdots <_1 y_{\beta_3} <_1 y_{\beta_2} <_1 y_{\beta_1} \tag{2}$$

where $y_{\beta_i}$ is chosen as above to satisfy

$$\beta_i \cong (<_1\langle y_{\beta_i}\rangle, <_1) \tag{3}$$

(2) contradicts the fact that $(Y, <_1)$ is a WO set (VI.2.13), and we have shown that $X$ has a minimal element, as long as we manage to convince that the inequalities in (2) indeed hold.

To this end, let $\beta < \gamma$ in $X$, where $\beta = (Z, <_2),\ \gamma = (W, <_3)$. We have

$$\gamma \cong (<_1 \langle y_\gamma\rangle, <_1) \tag{4}$$

and

$$\beta \cong (<_1 \langle y_\beta\rangle, <_1) \tag{5}$$

Also, by $\beta < \gamma$,

$$\beta \cong (<_3 \langle u\rangle, <_3), \qquad \text{where } u \in W \tag{6}$$

Observe that $y_\beta \neq y_\gamma$ (otherwise, $\beta \cong \gamma$ from (4) and (5), whence $\beta = \gamma$ by VI.4.6, contradicting $\beta < \gamma$ (irreflexivity)).

Assume now that $y_\gamma <_1 y_\beta$. Then $\gamma$, that is $(W, <_3)$, is isomorphic to a segment of $(<_1 \langle y_\beta\rangle, <_1)$ by (4), and therefore to a segment of $(<_3 \langle u\rangle, <_3)$ by (5) and (6). That is, $(W, <_3) \cong (<_3 \langle v\rangle, <_3)$, where $v <_3 u$, contradicting VI.3.16. Thus, $y_\beta <_1 y_\gamma$.

Let then $\beta$ be the $<$-minimal in $X$. We claim that $\beta$ is $<$-minimal (also $<$-minimum) in $A$, which will rest the case. Indeed, if not, then for some $\gamma$ in $A$, $\gamma < \beta$. Then $\gamma \in X$ by transitivity of $<$, contradicting the minimality of $\beta$ in $X$. □

**VI.4.13 Proposition (Informal Normal Form Theorem).** *For each* $\alpha \in \mathrm{On}$, $\{\beta : \beta < \alpha\} \cong \alpha$.

Since we have adopted the convention that lowercase Greek letters stand for ordinals, we will use the shorthand "$\{\beta : \ldots\}$" for "$\{\beta \in \mathrm{On} : \ldots\}$". Also, recall that – for now – $\alpha = (A, <_1)$ for some $A$ (set), so that the $<_1$-ingredient is incorporated in the notation "$\cdots \cong \alpha$". In writing "$\{\beta : \ldots\} \cong \cdots$", however, we are slightly abusing notation, since we ought to have written "$(\{\beta : \ldots\}, <) \cong \cdots$" instead, where $<$ is the order on On defined in VI.4.9. This type of notational abuse is common when the order is clearly understood (this echoes the remark following VI.3.3).

*Proof.* Let $\alpha = (Y, <_1)$ and $X = \{\beta : \beta < \alpha\}$.[†] As in the proof of VI.4.12, for each $\beta \in X$ we pick a $y_\beta \in Y$ such that

$$\beta \cong (<_1 \langle y_\beta \rangle, <_1) \tag{1}$$

Consider the relation $F = \{\langle \beta, y_\beta \rangle : \beta \in X\}$. It is single-valued in $y_\beta$, for if also $\beta \cong (<_1 \langle y'_\beta \rangle, <_1)$ and (without loss of generality) $y'_\beta <_1 y_\beta$, then

$$(<_1 \langle y'_\beta \rangle, <_1) \cong (<_1 \langle y_\beta \rangle, <_1)$$

contrary to VI.3.16.

We saw in the proof of VI.4.12 that $F$ is order-preserving ($\gamma < \beta \to y_\gamma <_1 y_\beta$); hence (by VI.3.8)

$$(X, <) \overset{F}{\cong} (\mathrm{ran}(F), <_1) \tag{2}$$

where $\mathrm{ran}(F) \subseteq Y$. Now, if $y \in Y$ and $\beta = \|(<_1 \langle y \rangle, <_1)\|$, then $\beta < \alpha$ by VI.4.9; hence $\beta \in X$ and $F(\beta) = y$. This shows that $F$ is onto $Y$. □

**VI.4.14 Proposition (The (Informal) Burali-Forti Antinomy).** On *is not a set.*

*Proof.* In the contrary case, (On, <) is a WO set, by VI.4.12. So let

$$\alpha = \|(\mathrm{On}, <)\|$$

Thus,

$$(\mathrm{On}, <) \cong \alpha \tag{1}$$

By VI.4.13,

$$(< \langle \alpha \rangle, <) \cong \alpha \tag{2}$$

(1) and (2) yield $(\mathrm{On}, <) \cong (< \langle \alpha \rangle, <)$, contradicting VI.3.16. □

[†] This is a different $X$ from the one employed in the proof of VI.4.12.

**VI.4.15 Remark.** The Burali-Forti antinomy is the first contradiction of naïve set theory, discovered by Burali-Forti (and Cantor himself). It is a "paradox" or "antinomy" in that it contradicts the thesis (Frege's) that for any formula of set theory, $\mathscr{F}(x)$, the class $\{x : \mathscr{F}(x)\}$ is a set. The $\mathscr{F}(x)$ in question here is "$x$ is an ordinal".

Observe, on the other hand, that by VI.4.13, by the fact that any $\alpha$ is some $(A, <_1)$ for some set $A$, and by collection, we have that $\{\beta : \beta < \alpha\} = <\langle\alpha\rangle$ is a set for any $\alpha$. In particular, this says that our tentative $<$ on On is left-narrow. □

By the normal form theorem (VI.4.13), $(\{\alpha : \alpha < \|(A, <_1)\|\}, <)$, where "$<$" is that of VI.4.9, is a member of $[(A, <_1)]_{\cong}$ for all $(A, <_1)$.

Let us ponder then what would be the consequences if the principle of global (strong) choice (invoked in VI.4.5) were to be so smart as to always pick

$$(\{\alpha : \alpha < \|(A, <_1)\|\}, <) \tag{$i$}$$

for "$\|(A, <_1)\|$", for *all* WO sets $(A, <_1)$. Since the order in all instances of $(i)$ is the same (that is, $<$ of VI.4.9), we could go one step further and just use the set $\{\alpha : \alpha < \|(A, <_1)\|\}$ as the ordinal for the WO set $(A, <_1)$, *implying*, rather than including explicitly, the order $<$. Of course, the sets in $(i)$ are $\cong$-invariants just as they are when thought of as WO sets under $<$. Under the pondered circumstances we end up with a recurrence

$$\|(A, <_1)\| \overset{\text{def}}{=} \{\alpha : \alpha < \|(A, <_1)\|\}$$

where the $\alpha$'s are the ordinals (according to our present speculative analysis) assigned to the segments of $(A, <_1)$ by VI.4.9.

The self-referential definition above, can also be written more simply as

$$< \langle\alpha\rangle = \alpha \tag{$ii$}$$

Let us "compute" (i.e., find which sets are) the first few ordinals. For example,[†] $(\emptyset, <_1)$ has *no* segments; therefore the set $\{\alpha : \alpha < \|(\emptyset, <_1)\|\}$ is empty, i.e.,

$$\|(\emptyset, <_1)\| = \emptyset, \qquad \text{the smallest ordinal}$$

Now, $(\{\emptyset\}, <_1)$ (where $<_1$ is empty as well) has one segment only, $(\emptyset, <_1)$. Hence, exactly one ordinal, $\emptyset$, is smaller than $\|(\{\emptyset\}, <_1)\|$. Thus

$$\|(\{\emptyset\}, <_1)\| = \{\emptyset\} \tag{$iii$}$$

[†] $<_1$ is the empty order here.

Next, let us compute $\|(\{a, b\}, <_2)\|$, where $a \neq b$ and $a <_2 b$. The only segments are $(\emptyset, <_2)$ and $(\{a\}, <_2)$, which have ordinals $\emptyset$ and $\{\emptyset\}$ respectively.

Of course, $(\{a\}, <_2) \cong (\{\emptyset\}, <_1)$; hence $\|(\{a\}, <_2)\| = \|(\{\emptyset\}, <_1)\| = \{\emptyset\}$ by $(iii)$. Thus,[†]

$$\|(\{a, b\}, <_2)\| = \|(\{\emptyset, \{\emptyset\}\}, <)\| = \{\emptyset, \{\emptyset\}\}$$

Note that for the first three ordinals, at least, their order $<$ coincides with $\in$, since

$$\emptyset \in \{\emptyset\} \in \{\emptyset, \{\emptyset\}\}$$

This is true of all ordinals, for[‡] $\beta \in \alpha$ iff (by $(ii)$) $\beta \in {<}\langle\alpha\rangle$ iff $\beta < \alpha$.

Continuing our pondering on what if global choice were smart, we observe that each ordinal is a *transitive set* (Definition V.1.11). Indeed, let $\alpha \in \beta \in \gamma$. By the previous remark this is equivalent to $\alpha < \beta < \gamma$; hence, by transitivity of $<$, $\alpha < \gamma$; therefore $\alpha \in \gamma$. Of course, an ordinal, being the set of all the smaller ordinals, will have as members only transitive sets.

Von Neumann showed that, surprisingly, these transitivity properties fully characterize the "appropriate concept" of an ordinal as a "special set", without any recourse to *any form* of AC – from which we disengage in the following "permanent" definition – and without any *a priori* reliance on the concept of well-ordering either.

The reader is now asked to consider all the preceding attempts to get ordinals off the ground as "motivational discussion" with a historical flavour. Therefore the definitions and consequences VI.4.2–VI.4.14 are to be discarded. Our formal study of ordinals starts with VI.4.16 below. In particular we will show that ordinals (as defined below) *are* $\cong$-invariants.

**VI.4.16 Definition.** (von Neumann.) An *ordinal*, or *ordinal number*, is a transitive set all of whose members are also transitive sets.

For the record, we may introduce a unary predicate "Ord" – which says of its argument that it is an ordinal – by the definition (1) below, where $T$ itself is the unary predicate introduced by $T(x) \leftrightarrow \neg U(x) \wedge (\forall y \in x)(\forall z \in y) z \in x$. $T(x)$ says that $x$ is a transitive set:

$$\text{Ord}(x) \leftrightarrow T(x) \wedge (\forall y \in x) T(y) \tag{1}$$

[†] $<$ here is that of VI.4.9.

[‡] By $(ii)$, the only members of ordinals – in the current stage of the tentative definition – are themselves ordinals. Thus "$x \in \alpha \wedge x \in \text{On}$" – that is, "$\beta \in \alpha$" – is equivalent to "$x \in \alpha$".

On will be the class of all ordinals; that is, On abbreviates the class term $\{x : \mathrm{Ord}(x)\}$. Lowercase Greek letters will denote arbitrary ordinals – that is, we employ, in our *argot*, "ordinal-typed" variables $\alpha$, $\beta$, $\gamma, \ldots$, with or without subscripts or primes, a notation that we extend to unspecified ordinal constants.

Thus in instances such as "$\ldots \alpha \ldots$" we will understand more: "$\ldots \alpha \wedge \alpha \in \mathrm{On} \ldots$". Of course, *specific* ordinals (i.e., specific ordinal constants) may have names deviating from this rule (e.g., $\emptyset$ in the lemma below). □

We now embark on developing the properties of ordinals.

**VI.4.17 Lemma.** $\mathrm{On} \neq \emptyset$.

*Proof.* $\emptyset$ satisfies Definition VI.4.16; therefore, $\emptyset \in \mathrm{On}$. □

**VI.4.18 Example.** Here are some more members of On, as the reader can readily verify using VI.4.16: $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}$, $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$.

Indeed, every natural number $n$, and the set of natural numbers $\omega$, are ordinals by V.1.12–V.1.13. □

The definition of ordinals does not explicitly state that the *members* of an ordinal are themselves ordinals. The following lemma says that.

**VI.4.19 Lemma.** *If* $x \in \alpha$*, then* $x \in \mathrm{On}$.

The above statement can be rephrased in a number of ways: "On is a transitive class", or "$\alpha \subseteq \mathrm{On}$ for all $\alpha$", or "every member of an ordinal is an ordinal". This last formulation coincides with the results of our earlier informal discussion.

*Proof.* Let

$$y \in x \in \alpha \tag{1}$$

By VI.4.16, $y \in \alpha$. Therefore (VI.4.16), $y$ is a transitive set. By VI.4.16 and (1), $x$ is transitive. Since so is its arbitrary member $y$, $x$ is an ordinal. □

**VI.4.20 Corollary (Normal Form Theorem).** $\{\beta : \beta \in \alpha\} = \alpha$.

*Proof.* For any set $y$, $y = \{x : x \in y\}$. In particular, $\alpha = \{x : x \in \alpha\}$. By VI.4.19,

$$\vdash_{\mathrm{ZFC}} x \in \alpha \leftrightarrow x \in \alpha \wedge x \in \mathrm{On}$$

Hence, $\alpha = \{x : x \in \alpha \wedge x \in \mathrm{On}\}$. Thus, using the notational convention of VI.4.16, we may write $\alpha = \{\beta : \beta \in \alpha\}$. □

Another way to say the above is "$\in\langle\alpha\rangle = \alpha$".

**VI.4.21 Theorem (Burali-Forti Antinomy).** On *is not a set.*

*Proof.* Suppose On is a set. By VI.4.19 it is an ordinal; hence On $\in$ On, which is impossible by foundation. □

**VI.4.22 Lemma.** $\in$ *restricted on On is a partial order with MC.*

"$\in$", as the context hopefully makes clear, is here the *relation* defined by the *predicate* "$\in$". We should not need to issue such warnings in the future.

*Proof.* That $\in$ has MC on On is trivial, since it does so on $\mathbb{U}_M$ (foundation). Next, $x \notin x$ for all sets, so that $\in$ is irreflexive. Finally, $\alpha \in \beta \in \gamma$ implies $\alpha \in \gamma$ by VI.4.16; hence $\in$ is transitive on On. □

**VI.4.23 Theorem.** $\in$ *well-orders* On.

*Proof.* By VI.4.22, it suffices to show that $\in$ is total on On. To this end, let

$$\mathscr{P}(\alpha, \beta) \quad \text{stand for} \quad \alpha \in \beta \vee \alpha = \beta \vee \beta \in \alpha \tag{0}$$

We will show that

$$(\forall\alpha)(\forall\beta)\mathscr{P}(\alpha, \beta) \tag{1}$$

where, of course, quantification is over On, as the "typed" variables $\alpha$ and $\beta$ make clear (cf. VI.4.16). We can prove (1) by $\in$-induction or, equivalently, by $\in$-MC. We do the latter. So let the negation of (1) hold (i.e., we argue by contradiction), that is, we add the assumption

$$(\exists\alpha)(\exists\beta)\neg\mathscr{P}(\alpha, \beta) \tag{2}$$

By $\in$-MC on On, let $\alpha_0$ be $\in$-minimal such that

$$(\exists\beta)\neg\mathscr{P}(\alpha_0, \beta) \tag{3}$$

Next, let $\beta_0$ be $\in$-minimal such that

$$\neg\mathscr{P}(\alpha_0, \beta_0) \tag{4}$$

Let now

$$\gamma \in \beta_0 \tag{5}$$

Then $\mathscr{P}(\alpha_0, \gamma)$ by (4) and $\in$-minimality of $\beta_0$. $\mathscr{P}(\alpha_0, \gamma)$ (by (0)) yields one of:

*Case 1.* $\alpha_0 = \gamma$. That is, (by (5)) $\alpha_0 \in \beta_0$, contradicting (4).

*Case 2.* $\alpha_0 \in \gamma$. By (5) and transitivity of $\beta_0$, again $\alpha_0 \in \beta_0$; unacceptable. We must therefore have

*Case 3.* $\gamma \in \alpha_0$.

Thus, by (5),

$$\beta_0 \subseteq \alpha_0 \tag{6}$$

Next, let

$$\delta \in \alpha_0 \tag{7}$$

Then $\in$-minimality of $\alpha_0$, and (3),[†] yield $\mathscr{P}(\delta, \beta_0)$. The latter yields in turn (by (0))

*Case 1.* $\delta = \beta_0$. That is, (by (7)) $\beta_0 \in \alpha_0$, contradicting (4).

*Case 2.* $\beta_0 \in \delta$. By (7) and transitivity of $\alpha_0$, again $\beta_0 \in \alpha_0$; unacceptable. This leaves

*Case 3.* $\delta \in \beta_0$.

Hence $\alpha_0 \subseteq \beta_0$, which along with (6) yields $\alpha_0 = \beta_0$. This contradicts (4). □

The above proof is essentially a duplicate of that for the trichotomy of $\in$ over the natural numbers (V.1.20), although here it covers a wider context. The reader may also wish to compare the above proof with that in Example VI.2.38.

**VI.4.24 Corollary.** $x \in \mathrm{On}$ *iff* $x$ *is a transitive set that contains no atoms as members, and* $\in$ *well-orders* $x$.

*Proof. Only-if part.* By VI.4.19, an ordinal $x$ satisfies $x \subseteq \mathrm{On}$. Thus, the restriction of the well-ordering $\in$ of On on $x$ well-orders the latter. Moreover, by VI.4.16 no atom is an ordinal; thus $y \in x \rightarrow \neg U(y)$.

*If part.* Let $x$ be a transitive set that contains no atoms, and let the restriction of $\in$ on $x$ be a well-ordering. Let $y \in x$. First off, $\neg U(y)$.

We need only show that $y$ is transitive. To this end let, in conjunctional notation,

$$u \in v \in y\,(\in x) \tag{1}$$

[†] $\neg(\exists\beta)\neg\mathscr{P}(\delta, \beta)$ follows; hence $(\forall\beta)\mathscr{P}(\delta, \beta)$; thus $\mathscr{P}(\delta, \beta_0)$ by specialization.

Applying transitivity of $x$ twice, we get in turn $v \in x$ and $u \in x$. Thus $\{u, v, y\} \subseteq x$. Since $\in$ is a well-ordering on $x$, it is also transitive on $x$. Hence, (1) yields that $u \in y$. But then $y$ is a transitive set. □

☡☡ It is a trivial observation that the corollary above goes through even if well-order(ing) were relaxed to total order(ing), as the reader can readily check. However the above "redundant" formulation is necessary if one desires to found the notion of ordinal *in the absence of the foundation axiom* (that axiom was used in VI.4.23 in an essential way). In that case one takes the statement of Corollary VI.4.24 as the *definition* of ordinals.

In this discussion, enclosed between double "dangerous turn" road signs, we digress to peek into this possible avenue of founding ordinals. This discussion is only of use in the proof of the *consistency of foundation with the remaining axioms of ZFC*, and can otherwise be omitted with no loss of continuity. So we temporarily suspend here (i.e., until the end of this "doubly dangerous" material) the axiom of foundation, and define:

**VI.4.25 Alternative Definition (Ordinals in ZF − Foundation).** $x$ is an *ordinal* iff it is a transitive atom-free set that is well-ordered by $\in$. The notational conventions of VI.4.16 will apply; in particular, we continue using the symbol "On" for the class of all ordinals. □

We have the following consequences, in point form:

(1) $\alpha \notin \alpha$ *for all ordinals*. (Careful here! We cannot rely on foundation to say that $\in$ is irreflexive.) Indeed, let

$$\alpha \in \alpha \tag{$i$}$$

Since (the right hand) $\alpha$ is (well-)ordered by $\in$,

$$\in \mid \alpha \text{ is irreflexive.} \tag{$ii$}$$

By $(i)$, the left $\alpha$ is a member of the right $\alpha$, so that $(ii)$ yields $\alpha \notin \alpha$ (these are two copies of the left $\alpha$). We have just contradicted $(i)$.

(2) $x \in \alpha \in \mathrm{On} \to x \in \mathrm{On}$. Assume $x \in \alpha \in \mathrm{On}$. As in the proof of the if part of VI.4.24, $x$ is a transitive set. By transitivity of $\alpha$, $x \subseteq \alpha$. At once we obtain that $x$ is atom-free, since $\alpha$ is. Moreover, $x$ is well-ordered by $\in$, an order inherited from $\alpha$. Thus, the alternate Definition VI.4.25 too implies that On is transitive, that is, ordinals only contain ordinals as members.

(3) $\alpha \subset \beta \to \alpha \in \beta$. Assume $\alpha \subset \beta$, and let $\gamma \in \beta - \alpha$ (set difference) be $\in$-minimum (we say *minimum* rather than *minimal* because $\in$ is total on $\beta$).

Therefore, if $\delta \in \gamma$; then $\delta \notin \beta - \alpha$. On the other hand, $\delta \in \beta$ by transitivity of $\beta$. Thus $\delta \in \alpha$; hence

$$\gamma \subseteq \alpha \tag{$iii$}$$

Next, let

$$\delta \in \alpha \tag{$iv$}$$

Since $\alpha \subset \beta$, we have $\delta \in \beta$. Moreover, $\gamma \in \beta$ as well; hence (since $\in$ is total on $\beta$) we have three cases:
*Case 1.* $\gamma = \delta$. This is untenable due to $\gamma \notin \alpha$ and $(iv)$.
*Case 2.* $\gamma \in \delta$. This is impossible as well, as it yields $\gamma \in \alpha$ by transitivity of $\alpha$ and $(iv)$. This leaves
*Case 3.* $\delta \in \gamma$. Along with $(iv)$, this yields $\alpha \subseteq \gamma$; hence $\alpha = \gamma$ by $(iii)$.
We conclude (using $=$, $\in$, $\subseteq$ conjunctionally) that

$$\alpha = \gamma \in (\beta - \alpha) \subseteq \beta$$

In short, $\alpha \in \beta$.

(4) $\alpha = \beta \vee \alpha \in \beta \vee \beta \in \alpha$. Let $\alpha \neq \beta$. Observe that $\alpha \cap \beta \subseteq \alpha$ and $\alpha \cap \beta \subseteq \beta$. Also, $\alpha \cap \beta$ is transitive (verify) and well-ordered by $\in$ (as a subset of $\alpha$) as well as atom-free (hence an ordinal). By hypothesis, one of the two inclusions ($\subseteq$) must be proper ($\subset$), in which case the other is equality. Indeed, if they are both proper, then, by (3), $\alpha \cap \beta \in \alpha$ and $\alpha \cap \beta \in \beta$; hence $\alpha \cap \beta \in \alpha \cap \beta$, contradicting (1). Say, $\alpha \cap \beta = \alpha$, i.e., $\alpha \subseteq \beta$. Since we have assumed $\alpha \neq \beta$, (3) yields $\alpha \in \beta$.

(5) $\alpha = \{\beta : \beta \in \alpha\}$. By (2).

(6) On *is well-ordered by* $\in$. We need only establish $\in$-MC on On. So let $\emptyset \neq A \subseteq \text{On}$, a subclass of On. Let $\alpha \in A$. If $\alpha \cap A = \emptyset$, then $\in \langle\alpha\rangle \cap A = \emptyset$, that is, $\alpha$ is $\in$-minimal in $A$. If now $\alpha \cap A \neq \emptyset$, then let $\beta$ be $\in$-minimal in $\alpha \cap A$ ($\alpha \cap A$ is a subset of the WO set $(\alpha, \in)$). We argue that $\beta$ is $\in$-minimal in $A$. If not, let $\gamma \in A$ be such that $\gamma \in \beta$. Then $\gamma \in \alpha$ by transitivity of $\alpha$; hence $\gamma \in \alpha \cap A$. This contradicts the choice of $\beta$.

This approach (sans foundation) may be considered attractive in that it relies on fewer axioms than that of VI.4.16. We are nevertheless committed to *having* foundation (which has already provided us with some interesting results in VI.2.38) and therefore will continue our development based on Definition VI.4.16.

**VI.4.26 Definition.** As is normal practice, we will often utilize the symbol "$<$" for the well-ordering $\in | \text{On}$. Thus $\alpha < \beta$ means exactly $\alpha \in \beta$. □

**VI.4.27 Lemma.** *The reflexive closure, $r_{On}(<) = \leq$, of $<$ coincides with $\subseteq$ on* On, *i.e., $\leq\ =\ \subseteq$ on* On.

*Proof.* Let $\alpha \leq \beta$. This means that $\alpha = \beta$ or $\alpha \in \beta$. In the former case, $\alpha \subseteq \beta$ is immediate. In the latter case it follows from the transitivity of $\beta$ ($\gamma \in \alpha \to \gamma \in \beta$).

Conversely, let $\alpha \subseteq \beta$. Since we want $\alpha = \beta \vee \alpha \in \beta$, by VI.4.23 we only need to discredit the hypothesis $\beta \in \alpha$. Well, that hypothesis, along with the original hypothesis, leads to $\beta \in \beta$. □

**VI.4.28 Example.** We already know that $\emptyset \in$ On. $\emptyset$ is the $<$-minimum element of On, since for any $\alpha$, $\emptyset \subseteq \alpha$ translates to $\emptyset \leq \alpha$. □

**VI.4.29 Remark.** By VI.4.20, $\alpha = \{\beta : \beta < \alpha\}$, or $\alpha = <\langle\alpha\rangle$, i.e., an ordinal is the set of all smaller ordinals. Thus, Definition VI.4.16, offered without the assistance of either AC or the concept of well-ordering, yields formally the property $(ii)$ of ordinals that we had arrived at in our wishful motivational discussion prior to VI.4.16. The next result will establish that ordinals are $\cong$-invariants of WO sets. Thus we have come now full circle, and all the pieces of the puzzle fit. □

**VI.4.30 Theorem.** *Let $(A, <_1)$ be a WO set. Then there is a unique ordinal $\alpha$ and a unique isomorphism $\phi_A$ for which*

$$(A, <_1) \overset{\phi_A}{\cong} (\alpha, <)$$

*where $<$ is the standard order $\in$ on* On.

*Proof.* By VI.3.20, and for the WO classes $(A, <_1)$ and (On, $<$),[†] we have these three alternatives:

(1) (On, $<$) is isomorphic to a segment of $(A, <_1)$. This is impossible, because collection would force On to be a set.
(2) (On, $<$) $\cong (A, <_1)$. Untenable, as in (1).
(3) So it must be that $(A, <_1) \cong (<\langle\alpha\rangle, <)$ for some $\alpha$. By VI.4.20 (cf. VI.4.29), this says

$$(A, <_1) \overset{\phi_A}{\cong} (\alpha, <) \qquad (i)$$

[†] Note that both $<_1$ and $<$ are left-narrow, the former because $A$ is a set, the latter by VI.4.20.

for some $\phi_A$. Suppose that $(A, <_1) \cong (\beta, <)$ as well, where (without loss of generality) $\beta < \alpha$, i.e., $\beta \in \alpha$. By $(i)$, $(\alpha, <) \cong (\beta, <)$; hence $(\alpha, <) \cong (<\langle\beta\rangle, <)$ contradicting VI.3.16. This settles uniqueness of $\alpha$.

By VI.3.19, $\phi_A$ is unique. □

**VI.4.31 Corollary.** $(\alpha, <) \cong (\beta, <)$ *iff* $\alpha = \beta$.

*Proof.* The if part is trivial. The only-if part was proved in the course of the above proof (uniqueness of $\alpha$). □

**VI.4.32 Remark.** (1) We can prove VI.4.30 without recourse to VI.3.20 by defining $\phi_A$ on $A$ by $<_1$-recursion as follows:[†]

$$\phi_A(a) = \{\phi_A(b) : b <_1 a\} \qquad \text{for all } a \in A$$

or

$$\phi_A(a) = \phi_A[<_1 \langle a\rangle] \tag{1}$$

The reader is asked to pursue this. Once successful, one can turn to *prove* VI.3.23 (for WO sets) using the theorem on the comparability of ordinals.

It is important to note that (1) is the *only* possible definition for $\phi_A$, for it is tantamount to the requirement that $\phi_A$ be an isomorphism, i.e., that

$$\phi_A(b) \in \phi_A(a) \quad \text{iff} \quad b <_1 a$$

(2) Whenever $(A, <_1) \cong (\alpha, <)$, we can intuitively think that the members of $\alpha$ serve as "indices" (or position names) for the ordering of the elements of $A$ in ascending order. $\alpha$ is the first index *not* needed in this "enumeration" of $A$. Compare this remark with the discussion that launched this section.

(3) With the normally accepted abuse of notation, we often write $\alpha \cong \beta$ to mean $(\alpha, <) \cong (\beta, <)$; thus Corollary VI.4.31 can be also stated as "$\alpha \cong \beta$ iff $\alpha = \beta$".

(4) Rephrasing VI.4.30, we can state that every $[(A, <_1)]_{\cong}$ contains a *unique ordinal WO set*, $(\alpha, <)$. We can then *re-introduce* the symbol $\|(A, <_1)\|$, formally this time, without any reliance *on any form of AC*, to mean $(\alpha, <)$, where $(A, <_1) \cong (\alpha, <)$. Actually, the following (final) definition picks just the ordinal $\alpha$ rather than the WO set $(\alpha, <)$. □

[†] We assume without loss of generality that $<_1$ has $A$ as its field; therefore we do not need to add "$\wedge\, b \in A$" to the condition $b <_1 a$.

**VI.4.33 Definition (Order Types of WO Sets).** For any WO set $(A, <_1)$, the symbol $\|(A, <_1)\|$ stands for the *unique* $\alpha$ which by VI.4.30 satisfies

$$(A, <_1) \cong (\alpha, \in)$$

$\alpha$ is called the *order type* of $(A, <_1)$. If $A$ is a set of *ordinals* and $<_1 \;=\; \in$, then we use the simpler notation $\|A\| = \alpha$ (rather than $\|(A, <_1)\| = \alpha$). □

**VI.4.34 Corollary.** $\|\alpha\| = \alpha$.

*Proof.* $(\alpha, <) \cong (\alpha, <)$ and VI.4.33. □

**VI.4.35 Corollary.** $(A, <_1) \cong (B, <_2)$ *iff* $\|(A, <_1)\| = \|(B, <_2)\|$.

*Proof. If part.* $(A, <_1) \cong \|(A, <_1)\| = \|(B, <_2)\| \cong (B, <_2)$.

*Only-if part.* $\|(A, <_1)\| \cong (A, <_1) \cong (B, <_2) \cong \|(B, <_2)\|$ and VI.4.31. □

**VI.4.36 Example.** Let $\emptyset \neq A$ be any class of ordinals (not just a set). Then $\bigcap A$ is a set. We will argue that it is an *ordinal*, indeed the *smallest* ($<$-minimum) ordinal in $A$.

Let $\alpha \in A$. Since $\bigcap A \subseteq \alpha$, $\bigcap A$ is well-ordered by $<$ (i.e., $\in$), and since none of $\alpha$ contains atoms (by VI.4.16), nor does $\bigcap A$. Using VI.4.24, we need only show that $\bigcap A$ is transitive in order to conclude that it is an ordinal.

So let $\beta \in \alpha \in \bigcap A$. Thus, $\gamma \in A \to \beta \in \alpha \in \gamma$. By transitivity of $\gamma$, $\gamma \in A \to \beta \in \gamma$; hence $\beta \in \bigcap A$.

Next,

$$\alpha \in A \to \bigcap A \subseteq \alpha \tag{1}$$

translates to (VI.4.27) $\alpha \in A \to \bigcap A \leq \alpha$. Thus, it only remains to prove that

$$\left(\bigcap A\right) \in A$$

or that *some among the inclusions* (1) *is an equality*. If not, by VI.4.27

$$\alpha \in A \to \left(\bigcap A\right) \in \alpha$$

Hence $\bigcap A \in \bigcap A$, a contradiction. □

## VI.5. The Transfinite Sequence of Ordinals

Ordinals have essentially been introduced in order to extend the natural number sequence, so that one can index, or number, elements of arbitrary WO sets.

Also, in much the same way that the natural numbers are employed to label *steps*, or *stages*, in a mathematical construction (by a recursive definition over $\omega$), ordinals can be used for the same purpose whenever the natural number sequence is not "long enough" for the labeling, or, in the case of a mathematical construction, whenever the stages of the construction are too many to be labelled by natural numbers. In this section we learn how to count (or how to sequence) with the help of ordinals, and find that ordinals are naturally split into three mutually exclusive types, namely, 0, limit ordinals, and successor ordinals. In the light of this classification we revisit, or rephrase, the principles of induction and recursive (inductive) definitions, already studied in Section VI.2 for arbitrary WO classes, as these principles apply over On or over an arbitrary $\alpha$. We will apply both induction and inductive definitions over On, under their new guise, in the next section to formally construct "all sets" starting from the urelements, and to study their properties. In particular, we will find there that the vague principle of "set formation by stages" – on which we have based the discovery, and "truth", of all the ZFC axioms except that of collection and infinity – can be made precise with the help of ordinals.

We recall here Definition V.1.1 of the set successor operation $x \cup \{x\}$ on any set $x$, and the notational convention established in V.1.19.

**VI.5.1 Definition (Successor on** On**).** The *successor* operation on sets $x$ is defined by $x \cup \{x\}$ and is generally denoted by $S(x)$.

If $x \in \mathrm{On}$, then $x + 1$ is a preferred synonym for $S(x)$. □

The notation $\alpha + 1$ for ordinals is consistent with that for the natural numbers (V.1.19). However, unlike the special case of natural numbers (which are "finite ordinals"), where $n + 1 = 1 + n$ is provable for the free variable $n$ over $\omega$ (cf. V.1.24), it is *not* the case that $\alpha + 1 = 1 + \alpha$ is provable in general. For example, we will soon see that $\vdash_{\mathrm{ZFC}} 1 + \omega \neq \omega + 1$. Of course, we have not yet said what "$1 + \alpha$" ought to mean in general, but that will be done soon.

We also recall here the result of Lemma V.1.9 and the fact (see remark prior to the proof) that

$$\vdash_{\mathrm{ZFC}} S(x) = S(y) \to x = y$$

for free $x$ and $y$, not just for variables restricted over $\omega$. In particular,

$$\vdash_{\mathrm{ZFC}} \alpha + 1 = \beta + 1 \to \alpha = \beta \qquad (1)$$

**VI.5.2 Example (What If?).** Let us prove (1) above again, this time without using foundation (which was used in V.1.9), but instead taking as independently given the fact that $<$, that is $\in$, on On is a total order (for example, this would have been the avenue taken if we were to omit the axiom of foundation and define ordinals as in the alternate definition VI.4.25).

Under such restrictions we still have trichotomy (see p. 336, item (4)), i.e., we have one of $\alpha = \beta,\ \alpha \in \beta,\ \beta \in \alpha$. So assume $\alpha + 1 = \beta + 1$, and let

$$\alpha \in \beta \tag{2}$$

Now, the hypothesis $\alpha \cup \{\alpha\} = \beta \cup \{\beta\}$ implies (via $\supseteq$) that $\beta \in \alpha$ or $\beta = \alpha$, either of which in turn implies, along with (2), that $\beta \in \beta$, contradicting the irreflexivity of the order $\in$ on On. Similarly, $\beta \in \alpha$ is untenable. This leaves $\alpha = \beta$. □

**VI.5.3 Lemma.** $\alpha + 1$ *is an ordinal.*

*Proof.* Let $y \in \alpha + 1 = \alpha \cup \{\alpha\}$. Then $y \in \alpha$ or $y = \alpha$; hence $y \in$ On in either case.

So every member of $\alpha + 1$ is transitive. Next, $x \in y \in \alpha + 1$ implies (as above) the cases $x \in y \in \alpha$ and $x \in y = \alpha$.

In either case $x \in \alpha$; hence $x \in \alpha + 1$. Thus $\alpha + 1$ is transitive too. □

**VI.5.4 Lemma.** $\vdash_{\mathrm{ZFC}} \alpha < \beta \leftrightarrow \alpha + 1 \leq \beta$.

*Proof.* $\leftarrow$: Let $\alpha \cup \{\alpha\} \subseteq \beta$ (translating "$\leq$" to "$\subseteq$" via VI.4.27). Then $\alpha \in \beta$.

$\rightarrow$: Let $\alpha \in \beta$. By transitivity of $\beta$, $\alpha \subseteq \beta$, which along with the hypothesis gives $\alpha \cup \{\alpha\} \subseteq \beta$. □

As a special case, we have $\vdash_{\mathrm{ZFC}} n < m \leftrightarrow n + 1 \leq m$, where $n, m$ are natural number variables.

**VI.5.5 Lemma.** $\vdash_{\mathrm{ZFC}} \alpha < \beta \leftrightarrow \alpha + 1 < \beta + 1$.

*Proof.* $\rightarrow$: Let $\alpha < \beta$. By VI.5.4, $\alpha + 1 \leq \beta$. But $\beta < \beta + 1$ (i.e., $\beta \in \beta \cup \{\beta\}$); hence $\alpha + 1 < \beta + 1$ (this formula simply says "$\beta < \beta + 1$" if $\alpha + 1 = \beta$; otherwise it follows from the transitivity of $<$ on On).

$\leftarrow$: Let $\alpha + 1 < \beta + 1$. Possible conclusions are $\beta < \alpha$, $\beta = \alpha$, or $\alpha < \beta$. The first option gives $\beta + 1 < \alpha + 1$ (by the $\rightarrow$-direction) and hence $\alpha + 1 < \alpha + 1$ by the hypothesis and transitivity, contradicting irreflexivity of $<$. The second option gives (Leibniz) $\beta + 1 = \alpha + 1$, again contradicting irreflexivity along with the assumption. It remains to take $\alpha < \beta$. □

As a special case, we have $\vdash_{\text{ZFC}} n < m \leftrightarrow n + 1 < m + 1$, where $n, m$ are natural number variables.

**VI.5.6 Lemma.** $\alpha + 1 \neq \emptyset$.

*Proof.* $\alpha \in \alpha + 1$. □

**VI.5.7 Remark.** Lemma VI.5.6 generalizes the case of natural numbers (V.1.8) to all ordinals.

From now on we will freely use the symbol 0 for $\emptyset$ in all contexts where the latter is thought of as an ordinal rather than just the empty set, since 0 is the symbol we have assigned to the smallest ordinal – the natural number 0 (V.1.19). □

As $\omega$ is an inductive set, indeed the $\subseteq$-smallest inductive set (V.1.5), it follows that whenever $n \in \omega$ then also $n + 1 \in \omega$; thus we cannot "reach" $\omega$ if we start at 0 and keep applying the successor operation. This makes $\omega$ a *limit* ordinal.

**VI.5.8 Definition.** A *limit ordinal* is an $\alpha$ such that

(1) $\alpha \neq 0$, and
(2) whenever $\beta \in \alpha$, then also $\beta + 1 \in \alpha$.

The notation "Lim($\alpha$)" says "$\alpha$ is a limit ordinal".

An ordinal $\alpha$ is a *successor ordinal*, or simply *successor*, just in case $\alpha = \beta + 1$ for some $\beta$. □

(1) Some authors allow 0 to be a limit ordinal (e.g., Jech (1978b)).
(2) Rephrasing VI.5.8, we can say (by V.1.1) that Lim($\alpha$) iff $\alpha$ is an inductive set.
(3) Every $n \in \omega$ such that $n \neq 0$ is a successor ordinal (V.1.10). So successor ordinals exist ($\{\emptyset\}$ and $\{\emptyset, \{\emptyset\}\}$, or 1 and 2, are two specific examples).
(4) If $\alpha = \beta + 1$, then $\beta$ is uniquely determined by $\alpha$ (by (1) on p. 340). We use the notation $\beta = \alpha - 1$ or $\beta = pr(\alpha)$ and call $\beta$ the *predecessor* of $\alpha$ (cf. V.1.15), but will not bother to introduce $pr$ on On formally.

**VI.5.9 Proposition.** *An ordinal is a successor ordinal iff it is a successor set.*

*Proof.* The only-if part is trivial.

*If part.* Say $x \cup \{x\} = \alpha$. Then $x \in \alpha$; hence $x = \beta$ for some $\beta$. □

**VI.5.10 Proposition.** *Limit ordinals exist.*

Translation: There is a set that is a limit ordinal.

*Proof.* By the axiom of infinity (V.1.3), it has already been established that $\omega$ is a set that is a limit ordinal. □

**VI.5.11 Theorem.** *Every $\alpha$ falls under exactly one of the following cases:*

(1) $\alpha = 0$,
(2) $\mathrm{Lim}(\alpha)$,
(3) *$\alpha$ is a successor.*

*Proof.* First, the cases are mutually exclusive. Indeed, (1) excludes (2) by definition, while it excludes (3) by VI.5.6. We verify that (2) excludes (3). Say $\mathrm{Lim}(\alpha)$, yet $\alpha = \beta + 1$ for some $\beta$. Then $\beta < \alpha$ and, by (2), $\beta + 1 < \alpha$ – i.e., $\alpha < \alpha$ – a contradiction (see also V.1.14).

Next, let $\alpha \neq 0$ and also $\neg\,\mathrm{Lim}(\alpha)$. Therefore, by trichotomy, for some $\beta < \alpha$ we have $\alpha \le \beta + 1$. By VI.5.4 and $\le\, = \,\subseteq$ on On, this yields $\alpha = \beta + 1$, thus $\alpha$ is a successor. □

Since On and any $\alpha$ are well-ordered by $<$, the results on induction and inductive definitions presented in Section VI.2 carry over with minor translations:

**VI.5.12 Theorem (Induction over On on Variable $\alpha$).** *To prove $(\forall\alpha)\mathscr{F}(\alpha)$ it suffices to prove, for arbitrary $\alpha$, that $\mathscr{F}(\alpha)$ follows from the induction hypothesis $(\forall\beta < \alpha)\mathscr{F}(\beta)$.*

Of course, "$(\forall\alpha)$" means "$(\forall\alpha \in \mathrm{On})$" (VI.4.16), while "for arbitrary $\alpha$" means that $\alpha$ is a free ordinal variable.

**VI.5.13 Theorem (Induction over $\delta$ on Variable $\alpha$).** *To prove $(\forall\alpha < \delta)\mathscr{F}(\alpha)$ it suffices to prove, for arbitrary $\alpha < \delta$, that $\mathscr{F}(\alpha)$ follows from the induction hypothesis $(\forall\beta < \alpha)\mathscr{F}(\beta)$.*

The general case of inductive definitions (VI.2.25) becomes:

**VI.5.14 Theorem (Recursive or Inductive Definitions over On).** *Let $\mathbb{G}$ be a (not necessarily total) function $\mathbb{G} : \mathrm{On} \times \mathbb{U}_M \to \mathbb{X}$, for some class $\mathbb{X}$. Then* *there exists a unique function* $\mathbb{F} : \mathrm{On} \to \mathbb{X}$ *satisfying*

$$(\forall\alpha)\mathbb{F}(\alpha) \simeq \mathbb{G}(\alpha, \mathbb{F} \restriction \alpha)$$

*Proof.* Recall that $<\langle\alpha\rangle = \alpha$. In particular, this makes $<$ over On left-narrow. □

**VI.5.15 Theorem (Recursive or Inductive Definitions over $\delta$).** *Let* $\mathbb{G}$ *be a (not necessarily total) function* $\mathbb{G} : \delta \times \mathbb{U}_M \to \mathbb{X}$*, for some class* $\mathbb{X}$*. Then there exists a unique function* $\mathbb{F} : \delta \to \mathbb{X}$ *satisfying*

$$(\forall\alpha \in \delta)\mathbb{F}(\alpha) \simeq \mathbb{G}(\alpha, \mathbb{F} \restriction \alpha)$$

Particularly useful is the translation of Corollary VI.2.31 in the context of On. We obtain two corollaries:

**VI.5.16 Corollary** (Pure **Recursion over** On)**.** *Let* $\mathbb{G}$ *be a (not necessarily total) function* $\mathbb{G} : \mathbb{U}_M \to \mathbb{X}$*, for some class* $\mathbb{X}$*. Then there exists a unique function* $\mathbb{F} : \mathrm{On} \to \mathbb{X}$ *satisfying*

(1) $(\forall\alpha)\mathbb{F}(\alpha) \simeq \mathbb{G}(\mathbb{F} \restriction \alpha)$*,*
(2) $\mathrm{dom}(\mathbb{F})$ *is either* On*, or some* $\alpha$*.*

**VI.5.17 Corollary** (Pure **Recursion over** $\delta$)**.** *Let* $\mathbb{G}$ *be a (not necessarily total) function* $\mathbb{G} : \mathbb{U}_M \to \mathbb{X}$*, for some class* $\mathbb{X}$*. Then there exists a unique function* $\mathbb{F} : \delta \to \mathbb{X}$ *satisfying*

(1) $(\forall\alpha \in \delta)\mathbb{F}(\alpha) \simeq \mathbb{G}(\mathbb{F} \restriction \alpha)$*,*
(2) $\mathrm{dom}(\mathbb{F})$ *is either* $\delta$*, or some* $\alpha < \delta$*.*

Theorem VI.5.11 leads to some additional interesting formulations of induction and inductive definitions over On (or over some $\delta$).

**VI.5.18 Theorem (Induction over** On **Rephrased).** *Let* $\mathbb{S} \subseteq \mathrm{On}$ *satisfy*

(1) $0 \in \mathbb{S}$*,*
(2) $(\forall\alpha)(\alpha \in \mathbb{S} \to \alpha + 1 \in \mathbb{S})$*,*
(3) *whenever* $\mathrm{Lim}(\alpha)$*, the hypothesis* $(\forall\beta < \alpha)\beta \in \mathbb{S}$ *implies* $\alpha \in \mathbb{S}$*.*

*Then* $\mathbb{S} = \mathrm{On}$*.*

*Proof.* Let instead $\mathbb{S} \neq \mathrm{On}$, and let $\alpha$ be the minimum element in $\mathrm{On} - \mathbb{S}$. By VI.5.11, $\alpha$ must be one of 0, a successor, or a limit ordinal.

Well, $\alpha \neq 0$ by (1). Next, $\alpha$ is not a successor either, for otherwise $\alpha - 1 \in \mathbb{S}$, hence $\alpha \in \mathbb{S}$ by (2).

Thus, perhaps $\mathrm{Lim}(\alpha)$. If so, by minimality of $\alpha$, $(\forall \beta < \alpha)\beta \in \mathbb{S}$. By (3) this entails $\alpha \in \mathbb{S}$, once more contradicting the choice of $\alpha$. So the hypothesis $\mathbb{S} \neq \mathrm{On}$ is untenable. □

Of course, the above can be rephrased in terms of a formula $\mathscr{S}(\alpha)$. The reader will easily carry out this translation by letting $\mathbb{S} = \{\alpha : \mathscr{S}(\alpha)\}$.

We offer two reformulations of inductive definitions over On, leaving the untold variations to the reader's imagination.

**VI.5.19 Theorem (Recursive or Inductive Definitions over** On **Rephrased).** *Let* $\mathbb{G}$ *and* $\mathbb{H}$ *be* (not necessarily total) *functions* $\mathrm{On} \times \mathbb{U}_M \to \mathbb{X}$ *and* $\mathrm{On} \times \mathbb{X} \to \mathbb{X}$ *respectively, for some class* $\mathbb{X}$*. Then there exists a unique function* $\mathbb{F} : \mathrm{On} \to \mathbb{X}$ *satisfying:*

(1) $\mathbb{F}(0) = x$ *(for some* $x \in \mathbb{X}$*),*
(2) $(\forall \alpha)\mathbb{F}(\alpha + 1) \simeq \mathbb{H}(\alpha, \mathbb{F}(\alpha))$*,*
(3) $(\forall \alpha)\big(\mathrm{Lim}(\alpha) \to \mathbb{F}(\alpha) \simeq \mathbb{G}(\alpha, \mathbb{F} \restriction \alpha)\big)$.

*Proof.* Define $\widetilde{\mathbb{G}} : \mathrm{On} \times \mathbb{U}_M \to \mathbb{X}$ by

$$\widetilde{\mathbb{G}}(\alpha, f) = \begin{cases} x & \text{if } \alpha = 0 \\ \mathbb{G}(\alpha, f) & \text{if } \mathrm{Lim}(\alpha) \\ \mathbb{H}(\alpha - 1, f(\alpha - 1)) & \text{if } \mathrm{dom}(f) \supseteq \alpha \wedge \alpha \text{ is a successor} \\ 0 & \text{otherwise} \end{cases}$$

Thus, by VI.5.11, (1)–(3) translate to $(\forall \alpha)\mathbb{F}(\alpha) \simeq \widetilde{\mathbb{G}}(\alpha, \mathbb{F} \restriction \alpha)$.

Note that by III.11.4 it is not necessary to add in the third case above "$\wedge\, f$ is a function", for $\mathrm{dom}(f)$ makes sense regardless. □

**VI.5.20 Theorem (Pure Recursive Definitions over** On **Rephrased).** *Let* $\mathbb{G}$ *and* $\mathbb{H}$ *be* (not necessarily total) *functions* $\mathbb{U}_M \to \mathbb{X}$ *and* $\mathbb{X} \to \mathbb{X}$ *respectively, for some class* $\mathbb{X}$*. Then there exists a unique function* $\mathbb{F} : \mathrm{On} \to \mathbb{X}$ *satisfying:*

(1) $\mathbb{F}(0) = x$ *(for some* $x \in \mathbb{X}$*),*
(2) $(\forall \alpha)\mathbb{F}(\alpha + 1) \simeq \mathbb{H}(\mathbb{F}(\alpha))$*,*
(3) $(\forall \alpha)\big(\mathrm{Lim}(\alpha) \to \mathbb{F}(\alpha) \simeq \mathbb{G}(\mathbb{F} \restriction \alpha)\big)$*,*
(4) $\mathrm{dom}(\mathbb{F})$ *is either* On*, or some* $\alpha$*.*

Let us now probe further into the ordinals.

**VI.5.21 Example.** (Refer to Example VI.2.34.) The support function $x \mapsto sp(x)$ is defined on all sets by the recursive definition[†]

$$sp(x) = \bigcup_{y \in x} sp(y) \tag{1}$$

By induction over On, assume for all $\beta < \alpha$ that $sp(\beta) = 0$. Thus, by (1), $sp(\alpha) = \bigcup_{\beta < \alpha} sp(\beta) = 0$. In sum

$$\vdash_{\mathrm{ZFC}} (\forall \alpha) sp(\alpha) = 0$$

i.e., all ordinals are *pure sets*. □

In view of the fact that the successor operation, $+1$, is inadequate to "reach" limit ordinals, we search for more powerful operations.

**VI.5.22 Theorem.** *Let* $A \subseteq \mathrm{On}$ *be a nonempty* set. *Then*

(1) $\bigcup A$ *is an ordinal,*
(2) $\alpha \leq \bigcup A$ *for all* $\alpha \in A$*,*
(3) $\bigcup A$ *is the* least *ordinal with property* (2).

*Proof.* (1): Let $x \in y \in \bigcup A$. Thus $x \in y \in \alpha$, for some $\alpha \in A$. Therefore $x \in \alpha$, and hence $x \in \bigcup A$, proving that $\bigcup A$ is transitive. On the other hand, from the above, since $y$ was arbitrary, we have that every element of $\bigcup A$ is an ordinal. This settles (1).

(2): This translates to $\alpha \subseteq \bigcup A$, which is trivial.

(3): Finally, let $(\forall \alpha \in A)\alpha \leq \delta$ for some $\delta$. That is, $(\forall \alpha \in A)\alpha \subseteq \delta$; hence $\bigcup A \subseteq \delta$. □

**VI.5.23 Definition.** Let $<$ be a partial order on $\mathbb{X}$, and $\mathbb{B} \subseteq \mathbb{X}$.

(1) $a \in \mathbb{X}$ is an *upper bound* of $\mathbb{B}$ iff $(\forall b \in \mathbb{B})b \leq a$. It is a *strict* upper bound iff $(\forall b \in \mathbb{B})b < a$.
(2) $c \in \mathbb{X}$ is a *least upper bound*, or *supremum*, of $\mathbb{B}$ iff it is an upper bound of $\mathbb{B}$ and for any upper bound $a$ of $\mathbb{B}$ we have $c \leq a$. □

**VI.5.24 Remark.**

(1) Suprema are unique, for if $c$ and $c'$ are suprema of $\mathbb{B}$, then $c \leq c'$ and $c' \leq c$, and hence $c = c'$ by antisymmetry. We write $c = \sup(\mathbb{B})$ or $c = \mathrm{lub}(\mathbb{B})$. Upper bounds with respect to the inverse order $>$ are called *lower bounds*

[†] $sp(x) = \{x\}$ on the assumption $U(x)$.

with respect to $<$. Correspondingly, least upper bounds with respect to $>$ are called *greatest lower bounds* or *infima* (singular *infimum*) with respect to $<$. The latter are also unique, and we write $d = \inf(\mathbb{B})$ or $d = \text{glb}(\mathbb{B})$ to indicate that $d$ is the infimum of $\mathbb{B}$ (in $(\mathbb{X}, <)$).

(2) If $\mathbb{B} = \emptyset$, then any $a \in \mathbb{X}$ is a lower bound, strict lower bound, upper bound, and strict upper bound of $\mathbb{B}$. Thus, the empty set has a supremum in $\mathbb{X}$ iff $\mathbb{X}$ has a $<$-*minimum* element (which, of course, is unique if it exists). Similarly, the statement "$\emptyset$ has a glb" is equivalent to "$\mathbb{X}$ has a $<$-*maximum* element". □

With the notation just introduced, Theorem VI.5.22 yields

**VI.5.25 Corollary.** *Let $A \subseteq \text{On}$, $A$ a set. Then* $\text{On} \ni \sup(A) = \bigcup A$.

Note that above, consistently with Remark VI.5.24, $A = \emptyset$ implies that its sup in On is 0. In other words, $\sup(A) = \bigcup A$ is valid for $A = \emptyset$.

**VI.5.26 Corollary.** *Let $\emptyset \neq A \subseteq \text{On}$, $A$ a set. Then*

(1) *The smallest ordinal* strictly *greater than all ordinals in $A$ is* $\sup\{\alpha + 1 : \alpha \in A\}$*, denoted by* $\sup^+(A)$.
(2) *If $A$ has a maximum element $\gamma$, then* $\sup(A) = \gamma$ *and* $\sup^+(A) = \gamma + 1$.
(3) *If $A$ does not have a maximum, then* $\sup(A) = \sup^+(A)$.

*Proof.* (1): By collection (cf. III.8.9), $B = \{\alpha + 1 : \alpha \in A\}$ is a set. By VI.5.22, $\sup^+(A) = \sup(B) = \bigcup B$ is the smallest ordinal such that

$$\alpha + 1 \le \sup^+(A) \qquad (i)$$

for all $\alpha \in A$. But $(i)$ is equivalent to $\alpha < \sup^+(A)$.

(2): Since $\alpha \le \gamma$ for all $\alpha \in A$, $\gamma$ is an upper bound of $A$; hence $\sup(A) \le \gamma$. But $\gamma \in A$ as well; hence $\gamma \le \sup(A)$. So $\sup(A) = \gamma$. For the rest, $\gamma + 1$ is trivially a *strict* upper bound of $A$. Let also $\delta$ be a strict upper bound. In particular, $\gamma < \delta$ (since $\gamma \in A$); hence $\gamma + 1 \le \delta$ by VI.5.4, establishing $\gamma + 1 = \sup^+(A)$.

(3): $\sup(A)$ is smallest satisfying

$$\alpha < \sup(A) \qquad (ii)$$

for all $\alpha \in A$, the "$\le$" becoming "$<$" due to the absence of a maximum element. But $\sup^+(A)$ also is smallest that satisfies $(ii)$, by (1) (regardless of the issue of maximum). Hence $\sup(A) = \sup^+(A)$. □

If $\emptyset \neq A \subseteq \mathrm{On}$ does not have a maximum, then $\sup(A)$ is a limit ordinal (see Exercise VI.14).

**VI.5.27 Definition (Transfinite Sequences).** A *transfinite sequence* is a function $f$ such that either $\mathrm{dom}(f) = \mathrm{On}$ or $\mathrm{dom}(f) = \alpha$ and $\omega < \alpha$. In the former case it is also termed an On-*sequence*, in the latter case an $\alpha$-*sequence*. □

As is usual, we think of $f$ as the "sequence" $(f(\delta))_{\delta<\alpha}$ – or $(f(\delta))_{\delta\in\mathrm{On}}$ if appropriate – and even write $(f_\delta)_{\delta<\alpha}$ or $(f_\delta)_{\delta\in\mathrm{On}}$. In the latter notation the argument $\delta$ becomes an *index* (or subscript), and $f_\delta$ is the *term* of the sequence at location (position) $\delta$. The concept of transfinite sequence derives from that of the familiar *finite* sequences (case where $\alpha < \omega$) and *infinite* sequences (case where $\alpha = \omega$). Intuitively, a transfinite sequence is just too "long" to be enumerated by natural numbers, and therefore it requires ordinals beyond natural numbers as indices for its terms.

**VI.5.28 Informal Definition.** A total $\mathbb{F} : \mathbb{A} \to \mathbb{B}$, where each of $\mathbb{A}$, $\mathbb{B}$ is equipped with a partial order, $<_1$, $<_2$ respectively, is:

(1) *Non-decreasing* or *monotone* just in case $\mathbb{F}(x) \leq_2 \mathbb{F}(y)$ whenever $x <_1 y$ in $\mathbb{A}$. If $<_1$ is $\in$ and $\mathbb{A} = \omega$, then $\mathbb{F}$ is an *ascending sequence*. The terminology derives from $\mathbb{F}(0) \leq_2 \mathbb{F}(1) \leq_2 \mathbb{F}(2) \leq_2 \cdots$.
(2) *Increasing* just in case it is order-preserving in the sense of VI.3.4, that is, $\mathbb{F}(x) <_2 \mathbb{F}(y)$ whenever $x <_1 y$ in $\mathbb{A}$.
(3) *Continuous* just in case, for each *nonempty set* $S \subseteq \mathbb{A}$, if $t = \sup(S)$, then $\sup(\mathbb{F}[S])$ exists and $\mathbb{F}(t) = \sup(\mathbb{F}[S])$.
(4) *Countably continuous* just in case for each ascending sequence $s : \omega \to \mathbb{A}$, if $t = \sup(\mathrm{ran}(s))$, then $\sup(\mathbb{F}[\mathrm{ran}(s)])$ exists and $\mathbb{F}(t) = \sup(\mathbb{F}[\mathrm{ran}(s)])$. More suggestively, we write this as $\mathbb{F}(\lim_n x_n) = \lim_n \mathbb{F}(x_n)$, where $x_n = s(n)$ for $n \in \omega$.

□

See also the discussion in VI.3.5.

"Continuity" here is a concept akin to continuity of functions of a real variable, if we interpret sup as a limit in the sense of calculus: Here sup commutes with the function letter, $\mathbb{F}(\sup(S)) = \sup(\mathbb{F}[S])$, exactly as $\lim_{x\to a}$ does in the case of limits in calculus.

Note that continuity implies quite a bit about the right field of $\mathbb{F}$ – In particular, the existence of suprema under certain conditions (that the sets considered are images under $\mathbb{F}$ of sets in $\mathbb{A}$ that themselves have suprema). On the other hand, if we independently know that, say, every nonempty sub*set* of $\mathbb{B}$ has a supremum (for example, a complete lattice does), then all that continuity of $\mathbb{F}$ adds is that the objects $\mathbb{F}(t)$ and $\sup(\mathbb{F}[S])$ are equal.

We define three additional concepts when $\mathbb{F}$ is a transfinite sequence.

**VI.5.29 Definition.** A transfinite sequence $f$ with $\operatorname{ran}(f) \subseteq \mathrm{On}$ is

(1) *weakly continuous* iff, for each $\alpha \in \operatorname{dom}(f)$, if $\operatorname{Lim}(\alpha)$ then $f(\alpha) = \sup\{f(\beta) : \beta < \alpha\}$,
(2) *normal* iff it is increasing and weakly continuous,
(3) *weakly normal* iff it is non-decreasing and weakly continuous. □

**VI.5.30 Proposition.** *A continuous function* $\mathbb{F}$*, as in* VI.5.28*, is non-decreasing.*

*Proof.* Let $x <_1 y$ in $\mathbb{A}$. Now, $\sup\{x, y\} = y$, hence $\sup\{\mathbb{F}(x), \mathbb{F}(y)\}$ exists and

$$\mathbb{F}(y) = \sup\{\mathbb{F}(x), \mathbb{F}(y)\}$$

(recall, $\mathbb{F}$ is total), i.e., $\mathbb{F}(x) \leq_2 \mathbb{F}(y)$. □

**VI.5.31 Corollary.** *A countably continuous function* $\mathbb{F}$*, as in* VI.5.28*, is non-decreasing.*

*Proof.* Let $x <_1 y$ in $\mathbb{A}$. Then

$$s = \lambda n.\begin{cases} x & \text{if } n = 0 \\ y & \text{if } n > 0 \end{cases}$$

is an ascending sequence and $\operatorname{ran}(s) = \{x, y\}$. □

**VI.5.32 Proposition.** *A continuous transfinite sequence $f$ with* $\operatorname{ran}(f) \subseteq \mathrm{On}$ *is weakly continuous.*

*Proof.* Let $\operatorname{Lim}(\alpha)$ and $\alpha \in \operatorname{dom}(f)$. Now, $\alpha = \sup\{\beta : \beta < \alpha\}$; hence, by continuity, $f(\alpha) = \sup\{f(\beta) : \beta < \alpha\}$. □

**VI.5.33 Corollary.** *A continuous transfinite sequence $f$ with* $\operatorname{ran}(f) \subseteq \mathrm{On}$ *is weakly normal.*

**VI.5.34 Corollary.** *An* increasing *continuous transfinite sequence $f$ with values in* On *is normal.*

The following establishes the converse of VI.5.33. It will prove useful in Section VI.10.

**VI.5.35 Proposition.** *If a transfinite sequence $f$ is weakly normal, then it is continuous.*

*Proof.* Let $\emptyset \neq S \subseteq \mathrm{On}$ be a set. Let $\alpha = \sup S$ (it exists by VI.5.22).

If $\alpha \in S$, then $f(\alpha) \in f[S]$ is maximum, since $f$ is non-decreasing.

Let $\alpha \notin S$. Then $\mathrm{Lim}(\alpha)$ by Exercise VI.14. Now

$$\sup f[S] = \bigcup\{f(\gamma) : \gamma \in S\} \subseteq \bigcup\{f(\gamma) : \gamma \in \alpha\} \tag{1}$$

since $\gamma \in S \rightarrow \gamma \in \alpha$. On the other hand, the choice of $\alpha$ yields

$$(\forall \gamma \in \alpha)(\exists \delta \in S)\gamma < \delta$$

Hence

$$(\forall \gamma \in \alpha)(\exists \delta \in S) f(\gamma) \leq f(\delta)$$

and the $\subseteq$ in (1) is promoted to equality. But the right hand side of $\subseteq$ is $f(\alpha)$ by weak continuity. □

**VI.5.36 Corollary.** *If $f$ is normal, then it is continuous.*

☡ **VI.5.37 Example.** A transfinite sequence $f$ can be weakly continuous without being continuous. This is because weak continuity can be satisfied by a function which is *not* non-decreasing. For example, let $f : \omega + 1 \rightarrow \omega + 1$ be given by

$$f(x) = \begin{cases} 2k & \text{if } x = 2k + 1 \wedge k \in \omega \\ 2k + 1 & \text{if } x = 2k \wedge k \in \omega \\ \omega & \text{if } x = \omega \end{cases}$$

Thus, $f(2k) = 2k + 1$ and $f(2k + 1) = 2k$ for all $k \in \omega$, so $f$ is not non-decreasing. On the other hand, $f(\omega) = \omega = \sup\{n : n < \omega\} = \sup\{f(n) : n < \omega\}$, and $\omega$ is the only limit ordinal in $\mathrm{dom}(f)$. □ ☡

So continuity of an $f : \mathrm{On} \rightarrow \mathrm{On}$ is equivalent to a (weak) monotonicity property, together with weak continuity. On the other hand, by the above example, weak continuity alone does not imply any monotonicity property for the function. It turns out that with a bit of a boost, weak continuity can imply a strong monotonicity property for the function, and hence continuity by VI.5.35.

**VI.5.38 Proposition.** *If $f$ is a weakly continuous* On*-sequence of ordinals that moreover satisfies* $(\forall\alpha)f(\alpha) < f(\alpha + 1)$*, then $f$ is increasing, and hence normal.*

*Proof.* We need to show $f(\alpha) < f(\beta)$ for all $\alpha < \beta$. We do induction on $\beta$.

*Basis.* $\beta = 0$. The contention is vacuously satisfied.

*The successor case.* Say $\beta = \gamma + 1$, and let $\alpha < \beta$. Thus, $\alpha = \gamma$ or $\alpha < \gamma$. In the former case, $f(\alpha) < f(\beta)$ by the assumption; in the latter case, by I.H., the assumption, and transitivity of $<$.

*The limit ordinal case.* Say $\mathrm{Lim}(\beta)$. By weak continuity,

$$f(\beta) = \sup\{f(\gamma) : \gamma < \beta\} \tag{1}$$

Let now $\alpha < \beta$, hence $\alpha + 1 < \beta$, so that

$$\begin{aligned} f(\alpha) &< f(\alpha + 1) && \text{by assumption} \\ &\le f(\beta) && \text{by (1)} \end{aligned}$$

Note that the I.H. was not needed in this case. □

**VI.5.39 Proposition.** *If $f$ is a weakly continuous* On*-sequence of ordinals that moreover satisfies* $(\forall\alpha)f(\alpha) \le f(\alpha + 1)$*, then $f$ is non-decreasing, and hence weakly normal.*

*Proof.* Exercise VI.16. □

The following easy result will be useful in Section VI.10. It says that a normal On-sequence of ordinals maps limit ordinals to limit ordinals.

**VI.5.40 Proposition.** *If $f$ is a normal* On*-sequence of ordinals and* $\mathrm{Lim}(\alpha)$*, then also* $\mathrm{Lim}(f(\alpha))$*.*

*Proof.* Suppose that $\mathrm{Lim}(\alpha)$. Then $f(\alpha) = \sup\{f(\gamma) : \gamma < \alpha\}$. But $f(\alpha) \notin \{f(\gamma) : \gamma < \alpha\}$ because $f$ is increasing. Thus $\mathrm{Lim}(f(\alpha))$ by Exercise VI.14. □

**VI.5.41 Definition (Fixed Points).** A *fixed point* (also called *fixpoint* sometimes) of a function $\mathbb{F} : \mathbb{A} \to \mathbb{A}$ is a $u \in \mathbb{A}$ such that $\mathbb{F}(u) = u$. □

**VI.5.42 Theorem (Knaster-Tarski).** *Let $(\mathbb{A}, <)$ be a PO class with a minimum element $t$, and where every ascending sequence has a supremum (meaning that its range does). If $\mathbb{F} : \mathbb{A} \to \mathbb{A}$ is countably continuous, then $\mathbb{F}$ has a fixed point.*

*Proof.* Define by recursion over $\omega$ the sequence $(s_n)_{n<\omega}$ by

$$\begin{aligned} s_0 &= t \\ s_{n+1} &= \mathbb{F}(s_n) \end{aligned}$$

By induction on $n$ one sees that the sequence is ascending. Indeed, $t = s_0 \le s_1$ ($t$ is minimum), and if (I.H.) $s_n \le s_{n+1}$, then, by VI.5.31, $s_{n+1} = \mathbb{F}(s_n) \le \mathbb{F}(s_{n+1}) = s_{n+2}$.

Let $u = \sup\{s_n : n < \omega\}$. By countable continuity,

$$\begin{aligned} \mathbb{F}(u) &= \sup\{\mathbb{F}(s_n) : n < \omega\} \\ &= \sup\{s_{n+1} : n < \omega\} && (1) \\ &= \sup\{s_n : n < \omega\} && (2) \\ &= u \end{aligned}$$

where the passage from (1) to (2) is justified by $s_0 \le s_n$ for all $n \in \omega$. □

**VI.5.43 Corollary.** *The fixed point $u$ of the previous theorem is* $\le$-least. *That is, any $c$ such that $\mathbb{F}(c) \le c$ satisfies $u \le c$.*

In particular, any $c$ such that $\mathbb{F}(c) = c$ satisfies $u \le c$.

*Proof.* Let $\mathbb{F}(c) \le c$. Now, by induction on $n$ we see that $s_n \le c$ for all $n < \omega$, because $s_0 = t \le c$, and if (I.H.) $s_n \le c$, then $s_{n+1} = \mathbb{F}(s_n) \le \mathbb{F}(c) \le c$.

Thus $u = \sup\{s_n : n < \omega\} \le c$. □

**VI.5.44 Corollary.** *If $f$ is a weakly normal transfinite* On*-sequence, then it has a fixed point $\beta$.*

*Proof.* The proof follows that of Theorem VI.5.42. We must just ensure that the key assumptions hold. Well, On has a minimum element, and if $(s_n)_{n<\omega}$ is ascending, then $\sup\{s_n : n < \omega\}$ exists by VI.5.22. The rest is taken care of by VI.5.35. □

**VI.5.45 Corollary.** *If $f$ is a normal transfinite* On*-sequence, then, for every $\gamma$, it has a fixed point $\beta$ such that $\gamma < \beta$.*

*Proof.* All else is as above, but now define $s_0 = \gamma + 1$. You will need to argue that $(s_n)_{n<\omega}$ is non-decreasing via a different route than before (Exercise VI.18). □

The above says that normal On-sequences of ordinals have *arbitrarily large* fixed points.

It is easy to see that the proof (imitating that of the theorem) yields the *least fixed point* greater than $\gamma$ (Exercise VI.18).

Theorem VI.5.42 can be sharpened in one direction, that is, dropping the requirement of (countable) continuity. A small trade-off towards achieving this is to restrict attention to PO *sets* $(A, <)$ where every subset of $A$ – not just ascending sequences – has a supremum in $A$.

**VI.5.46 Definition.** Let $(A, <)$ be a PO set. A total function $f : A \to A$ is *inclusive* or *expansive* iff, for all $x \in A$, $x \leq f(x)$. □

The terminology depends on which side of $\leq$ one is looking at. The input is "expanded" by, or "included"[†] in, the output.

**VI.5.47 Theorem.** *Let $(A, <)$ be a PO set such that every $S \subseteq A$ has a least upper bound in A. If $f : A \to A$ is either inclusive or monotone, then it has a fixpoint $c \in A$, that is, $f(c) = c$.*

*Proof.* Let $t = \sup \emptyset$, the minimum element of $A$. We define, by recursion over On, the transfinite sequence $s : \mathrm{On} \to A$:

$$s_\alpha = f\big(\sup\{s_\beta : \beta < \alpha\}\big) \tag{1}$$

$\alpha \mapsto s_\alpha$ is total on On. For convenience we set

$$s_{<\alpha} = \sup\{s_\beta : \beta < \alpha\} \tag{2}$$

This simplifies (1):

$$s_\alpha = f(s_{<\alpha}) \tag{3}$$

We now claim that $\alpha \mapsto s_\alpha$ is monotone.

[†] It is no more weird to pronounce $a \leq b$ – where $\leq$ is an arbitrary order – "$a$ is included in $b$" than to pronounce it "$a$ is less than or equal to $b$". Each version has an obvious "concrete" motivation.

*Case 1. $f$ is inclusive.* Then $s_{<\alpha} \leq s_\alpha$ by (3); hence $s_\beta \leq s_\alpha$ whenever $\beta < \alpha$ (by (2)).

*Case 2. $f$ is monotone.* By (2), $\beta < \alpha$ implies $s_{<\beta} \leq s_{<\alpha}$. Hence, by monotonicity, $f(s_{<\beta}) \leq f(s_{<\alpha})$. That is, $s_\beta \leq s_\alpha$.

By collection, $\lambda\alpha.s_\alpha$ cannot be 1-1 ($A$ is a set). Let us fix attention on some $\beta$ and $\gamma$ such that $\beta < \gamma$ and $s_\beta = s_\gamma$. By monotonicity of $\lambda\alpha.s_\alpha$, if $\beta < \alpha < \gamma$ then $s_\beta = s_\alpha$; thus

$$s_{<\gamma} = \sup\{s_\alpha : \alpha < \gamma\} = s_\beta \tag{4}$$

We can now calculate as follows:

$$\begin{aligned} s_\beta &= s_\gamma \\ &= f(s_{<\gamma}) \\ &= f(s_\beta), \qquad \text{by (4)} \end{aligned}$$

Thus, $c = s_\beta$ works. □

**VI.5.48 Remark.** (1) The reader can easily verify that we can weaken somewhat the assumption on $(A, <)$ and still prove our theorem. It suffices to postulate that the PO set has a supremum for every *chain*.[†] Thus, (1) would be undefined unless $\{s_\beta : \beta < \alpha\}$ is a chain. Well, one has to prove that it will be a chain (under the changed assumptions for $(A, <)$) anyway (Exercise VI.19).

(2) It turns out that with the $\beta$ and $\gamma$ as fixed in the proof above,

$$\gamma \leq \alpha \rightarrow s_\gamma = s_\alpha \tag{5}$$

On can prove (5) by induction, since the class of ordinals above $\gamma$ is well-ordered. Thus assume the claim for all $\alpha$ such that $\gamma \leq \alpha < \delta$. Now, monotonicity of $\lambda\alpha.s_\alpha$ and the I.H. entail

$$s_{<\delta} = \sup\{s_\theta : \theta < \delta\} = s_\gamma \tag{6}$$

Applying $f$ to the two extreme sides of (6) and remembering that $s_\gamma$ is a fixpoint of $f$, we obtain $s_\delta = s_\gamma$. In particular, *for the $\gamma$ that we fixed in the proof*, we have shown that $s_\gamma = s_{<\gamma}$.

**Pause.** Must it also be the case, for the $\beta$ of the proof, that $s_{<\beta} = s_\beta$? □

**VI.5.49 Corollary.** *Restricting the assumptions of* VI.5.47 *to a monotone $f : A \rightarrow A$, there is a* least *fixpoint $c$ for $f$. That is, $f(c) = c$, and if $f(d) \leq d$, then $c \leq d$.*

[†] That is, every set $S \subseteq A$ that is totally ordered by $<$.

*Proof.* The $c$ of the proof of VI.5.47 works. It suffices to prove that $s_\alpha \leq d$ for all $\alpha$.

For $\alpha = 0$, $s_0 = f(\sup \emptyset)$. Now, $\sup \emptyset \leq d$; hence $s_0 = f(\sup \emptyset) \leq f(d) \leq d$, using monotonicity of $f$. In general, $s_{<\alpha} = \sup\{s_\delta : \delta < \alpha\} \leq d$ by I.H. By monotonicity, $s_\alpha = f(s_{<\alpha}) \leq f(d) \leq d$. □

We conclude this section with the important *Zermelo well-ordering principle* and another theorem that is equivalent to AC. The connection here is that the proofs involve recursively defined transfinite sequences.

**VI.5.50 Theorem (Zermelo's Well-Ordering Principle).** *Every set can be well-ordered.*

*Proof.* Let $x$ be any set. If $x = \emptyset$, then the result is trivial. Assume then that $x \neq \emptyset$ and let $f$ be a choice function (AC) on $\mathbf{P}(x) - \{\emptyset\}$, i.e.,

$$(\forall y)\bigl(\emptyset \neq y \subseteq x \to f(y) \in y\bigr) \tag{1}$$

By recursion over On (with $\alpha$ as the recursion variable) define

$$(\forall \alpha) h(\alpha) \simeq f\bigl(x - \operatorname{ran}(h \restriction \alpha)\bigr) \tag{2}$$

It follows by VI.5.16 ((2) is a pure recursion) that $\operatorname{dom}(h) = \mathrm{On}$, or $\operatorname{dom}(h) = \gamma$ for some $\gamma$. Now, $h$ is 1-1, for if $\alpha < \beta$ and $\beta \in \operatorname{dom}(h)$ – so that $\alpha \in \operatorname{dom}(h)$ as well – then, by (1) and (2), $h(\beta) \in x - \operatorname{ran}(h \restriction \beta)$, and hence $h(\beta) \neq h(\alpha)$. Thus, by collection – since $\operatorname{ran}(h) \subseteq x$ – we have $\operatorname{dom}(h) = \gamma$.

$h$ is onto $x$, for $\operatorname{dom}(h) = \gamma$ entails that

$$\begin{aligned}\gamma &= \min\{\delta : \delta \notin \operatorname{dom}(h)\}\\ &= \min\bigl\{\delta : f\bigl(x - \operatorname{ran}(h \restriction \delta)\bigr)\uparrow\bigr\}\\ &= \min\{\delta : x - \operatorname{ran}(h \restriction \delta) = \emptyset\}\end{aligned}$$

That is, $x = \operatorname{ran}(h \restriction \gamma) = \operatorname{ran}(h)$.

By VI.3.12, $h$ induces a well-ordering $<_1$ on $x$ such that $\|(x, <_1)\| = \gamma$. □

**VI.5.51 Remark.** The above theorem is due to Zermelo (1904, 1908). The proof in his 1904 paper is reproduced in Kamke (1950) (see also Exercise IV.3). It is noteworthy that while AC was, of course, employed in an essential way in the original proof, it was taken there to be a "fundamental truth" of set theory[†] rather than an additional assumption (axiom).

[†] See Kamke (1950, p. 112), especially the concluding remarks prior to the statement of the well-ordering theorem.

Cantor had conjectured (but not proved) a special case of the well-ordering theorem in 1883, where $x$ is the set of reals, $\mathbb{R}$. □

We have remarked several times that AC holds on any WO set. Thus,

**VI.5.52 Corollary.** *AC is equivalent to the well-ordering principle (in the presence of the remaining axioms).*

*Proof.* If $F$ (a set) is a family of nonempty sets, then let $<_1$ well-order $\bigcup F$. To each $x \in F$ associate its $<_1$-minimum element $x_{\min}$. The function $x \mapsto x_{\min}$ is a choice function on $F$. □

The careful reader will observe that "remaining axioms" need *not* include foundation or power set, as the ordinals can be developed without these axioms.

**VI.5.53 Corollary.** *AC is equivalent to the following: For every set $x$ there is an ordinal $\alpha$ and a function $g$ with* $\mathrm{dom}(g) = \alpha$ *and* $x \subseteq \mathrm{ran}(g)$.

*Proof.* Assume AC. Let $x \neq \emptyset$. Referring to the proof of VI.5.50, we can take $g = h$ and $\alpha = \gamma$. If $x = \emptyset$, then $\alpha = 1$ and $g = \{\langle 0, 0\rangle\}$ work.

Conversely, let $F$ be a nonempty family of nonempty sets. We take $x = \bigcup F$ and let $\alpha$ and $g$ be as described in the corollary.

A choice function for $F$ is $\lambda y.g\Big(\min(g^{-1}[y])\Big) : F \to x$. □

The following is important for the next chapter.

**VI.5.54 Corollary.** *For every set $x$ there is an ordinal $\alpha$ and a* 1-1 *correspondence between $x$ and $\alpha$.*

**VI.5.55 Theorem (Kuratowski-Zorn Theorem).** *If $(A, <)$ is a PO set where every chain has an upper bound, then for every $a \in A$ there is a $<$-maximal element $c \in A$ such that $a \leq c$.*

The above is usually referred to as "Zorn's lemma ".

*Proof.* Let $f$ be a choice function on $\mathbf{P}(A) - \{\emptyset\}$. We define by recursion a transfinite sequence $\lambda\alpha.t_\alpha$:

$$\begin{aligned} t_0 &= a \\ t_{\alpha+1} &\simeq f\big(\{x : t_\alpha < x\}\big) \\ t_\alpha &\simeq f\Big(\big\{x : x \text{ is an upper bound of } \{t_\beta : \beta < \alpha\}\big\}\Big) \qquad \text{if } \mathrm{Lim}(\alpha) \end{aligned} \tag{1}$$

(1) is a pure recursion; thus, $\mathrm{dom}(\lambda\alpha.t_\alpha) = \mathrm{On}$ or $\mathrm{dom}(\lambda\alpha.t_\alpha) = \theta$ for some $\theta \in \mathrm{On}$. We will determine which one is the case.[†] Let us simply write "$t$" for the function $\lambda\alpha.t_\alpha$. We prove that $t$ is increasing on $\mathrm{dom}(t)$, that is,[‡]

$$\alpha < \beta \in \mathrm{dom}(t) \to t_\alpha < t_\beta \tag{2}$$

We do induction on $\beta$ (the proof is entirely analogous to that of VI.5.38).

For the basis, the implication (2) is trivially provable if $\beta = 0$. Suppose now that $\beta = \gamma + 1$. There are two cases:

One is where $\alpha = \gamma$, and we are done by the second case in (1).

The other is where $\alpha < \gamma$. The I.H. yields $t_\alpha < t_\gamma$. But we also have $t_\gamma < t_{\gamma+1}$ by (1). We are done by transitivity of $<$.

Finally, let $\mathrm{Lim}(\beta)$. As remarked in the preceding footnote, $\alpha < \beta$ implies $\alpha \in \mathrm{dom}(t)$. Since $t_\beta \downarrow$, the third case in (1) yields that $t_\alpha \leq t_\beta$ for any $\alpha < \beta$. For such an $\alpha$, $\alpha + 1 < \beta$ as well; thus $\alpha + 1 \in \mathrm{dom}(t)$ and $t_{\alpha+1} \leq t_\beta$. But $t_\alpha < t_{\alpha+1}$ by the second case in (1).

We must thus choose the case $\mathrm{dom}(t) = \theta$ by collection. We claim that $\theta$ is a successor (it is not 0, since $t_0 = a$). If not, $\mathrm{Lim}(\theta)$. But then, $\{t_\alpha : \alpha < \theta\}$ is a chain because $t$ is increasing, thus $t$ is defined at $\theta$ using the third case of (1), contradicting the fact that $\mathrm{dom}(t) = \theta$.

Let then $\theta = \eta + 1$. Then $t_\eta \downarrow$ and $a \leq t_\eta$ (why "$\leq$" and not "$<$"?). Moreover, $t_\eta$ is $<$-maximal; otherwise the second case in (1) would define $t_{\eta+1}$. □

**VI.5.56 Corollary (Hausdorff's Theorem).** *In a PO set $(A, <)$ every chain $B \subseteq A$ is included in some maximal chain $C$. That is, $C$ is a chain, $B \subseteq C$, and there is no chain $D$ such that $C \subset D$.*

*Proof.* Let us order the set of $<$-chains of $A$ by inclusion. So we have $<$-chains and $\subseteq$-chains.

[†] Note that (1) may yield undefined right hand sides in the second or third case of the definition, because the set we are using as the argument of $f$ is actually not in the domain of $f$ (because it is $\emptyset$). For example, this may happen in the third case if $\{t_\beta : \beta < \alpha\}$ is not a chain.

[‡] Since $\mathrm{dom}(t)$ is On or an ordinal, it is transitive. Therefore, $\alpha \in \beta \in \mathrm{dom}(t)$ implies $\alpha \in \mathrm{dom}(t)$.

Now, the union of the members of a $\subseteq$-chain – these are $<$-chains – is a $<$-chain. Indeed, let $S$ be a $\subseteq$-chain, and let $x \in \bigcup S$ and $y \in \bigcup S$. Then $x \in B \in S$ and $y \in B' \in S$. Without loss of generality let $B \subseteq B'$. Then $x$ and $y$ are in $B'$ and thus are $<$-comparable. In short, $\bigcup S$ is a $<$-chain. It is trivially a $\subseteq$-upper bound of the members of $S$ ($<$-chains).

It follows by VI.5.55 that for any $<$-chain $B$ there is a $\subseteq$-maximal $<$-chain $C$ such that $B \subseteq C$. □

**VI.5.57 Corollary.** *Hausdorff's theorem is equivalent to Zorn's lemma, and thus to AC.*

*Proof.* In view of the proof of VI.5.56, we need only prove that the latter implies Zorn's lemma. Let then $(A, <)$ be a PO set where every chain has an upper bound. Let $a \in A$. Now, $\{a\}$ is a chain; thus there is a maximal chain $C \subseteq A$ such that $a \in C$. Let $c$ be an upper bound of $C$. Then $a \leq c$ trivially. Moreover, $c$ is maximal, for if not, there is a $b > c$. But then $C \cup \{b\}$ is a chain that properly extends $C$. □

We have learnt a few of the properties of the transfinite sequence of ordinals in this section, some of which will be conveniently used in the sequel, especially in Section VI.10. There is a bit more that we will have to say in the latter section. For the whole story, the advanced and curious reader should consult Levy (1979) and the older references Bachmann (1955), Sierpiński (1965).

## VI.6. The von Neumann Universe

We now turn to formalizing "stages" of set construction within set theory, and to studying what such formalization entails. We will define a transfinite sequence of sets – built from an arbitrarily chosen set of urelements $N$ – which when taken together constitute a "universe" of sets and atoms of set theory built from $N$, in the sense that all axioms of set theory hold in this universe. This construction is effected within ZFC by recursion on ordinals, and for every $\alpha$ formally yields a *set*, $V_N(\alpha)$, that consists of all sets (and atoms) that we can define at "stage" $\alpha$. The (proper) class $\mathbb{U}_N = \bigcup_{\alpha \in \mathrm{On}} V_N(\alpha)$ is all we can construct from the atoms $N$, using the axioms.

If we mimic the formal construction outside ZFC, using "real" mathematical objects for atoms and working within "real" mathematics, we may then Platonistically proclaim that we have, at long last, constructed *the* "natural" model of set theory, a model that we have only vaguely described in II.1.3.[†]

[†] But from which vague description we have firmly justified the selection of axioms of ZFC!

The reader is cautioned that the formal construction within ZFC does not provide a formal proof of consistency of the axioms. What it does is build a formal interpretation of $L_{\text{Set}}$ and ZFC over the language $L_{\text{Set}}$ and ZFC. Thus, *formally*, it only proves that (cf. I.7.10) if ZFC is consistent, then ZFC is consistent.[†] Hardly newsworthy. Nevertheless, as we have noticed above, Platonistically we get much more out of this construction.

**VI.6.1 Definition (The Cumulative Hierarchy** or **von Neumann Universe).** Recall that we have been using the (rather unimaginative) name $M$ formally, having introduced it by the formal definition

$$M = y \leftrightarrow \neg U(y) \wedge (\forall x)\big(x \in y \leftrightarrow U(x)\big)$$

or simply put, $M = \{x : U(x)\}$. For any $N \subseteq M$ we define $V_N(\alpha)$ by induction over On by

$$\begin{aligned} V_N(0) &= N \\ V_N(\alpha + 1) &= \mathbf{P}(N \cup V_N(\alpha)) \\ V_N(\alpha) &= \textstyle\bigcup_{\beta<\alpha} V_N(\alpha) \qquad \text{if } \operatorname{Lim}(\alpha) \end{aligned}$$

If $N = \emptyset$, then we omit the subscript "$N$" in $V_N(\alpha)$ and just write $V(\alpha)$.

We also define the sequence $R_N(\alpha)$ by

$$\begin{aligned} R_N(0) &= \emptyset \\ R_N(\alpha + 1) &= \mathbf{P}(N \cup R_N(\alpha)) \\ R_N(\alpha) &= \textstyle\bigcup_{\beta<\alpha} R_N(\alpha) \qquad \text{if } \operatorname{Lim}(\alpha) \end{aligned}$$

If $N = \emptyset$, then we omit the subscript "$N$" in $R_N(\alpha)$ and just write $R(\alpha)$.

We denote $\bigcup_{\alpha\in\text{On}} R_N(\alpha)$ the class of *well-founded sets built from* $N$, by $\mathbf{WF}_N$. □

**VI.6.2 Remark.** We view the above as a recursive definition of the functions $\lambda\alpha.V_N(\alpha)$ and $\lambda\alpha.R_N(\alpha)$, effected for any set $N$ of urelements. We can also view it as defining $\lambda\alpha N.V_N(\alpha)$ and $\lambda\alpha N.R_N(\alpha)$ respectively, i.e., where $N$ is a parameter. We then explicitly arrange that the right hand side in each case is equal to a "don't care value" if $N \subseteq M$ fails. We can use $\emptyset$ for this value.

Alternatively, we may define $\lambda\alpha A.V_A(\alpha)$ for any set $A$ (parameter) but modify the definition setting $V_A(0) = TC(A)$ and $V_A(\alpha+1) = \mathbf{P}(TC(A) \cup V_N(\alpha))$.

One can easily prove by induction on $\alpha$ that $sp(V_N(\alpha)) \subseteq N$.

[†] We actually end up deriving a somewhat less trivial result.

In what follows we want to (*formally*) settle two claims:

One, that $\bigcup_{\alpha\in\mathrm{On}} V_N(\alpha)$, for any initial set of urelements $N$, satisfies all axioms of set theory. Or, Platonistically, that this union is a "universe" of sets and atoms (built from $N$).

Two, that $\bigcup_{\alpha\in\mathrm{On}} V_N(\alpha)$ contains *all* the *objects* (i.e., sets and urelements) of set theory, if these objects are built from the initial set of atoms $N$, i.e., that $\bigcup_{\alpha\in\mathrm{On}} V_N(\alpha) = \{x : sp(x) \subseteq N\}$. Even though this will be done formally, we want to point out its Platonist interpretation: If our recursive definition is carried out in the realm of real mathematics, and if $N$ happens to contain all the atoms, then $\bigcup_{\alpha\in\mathrm{On}} V_N(\alpha)$ contains *everything*: it is the class of all mathematical objects, $\mathbb{U}_N$.

The above inductive definition reflects the intuitive idea of the formation of sets by stages. At stage 0 we collect a collection of atoms, which are given outright, into a set via the equation $V_N(0) = N$. Subsequently, urelements are used along with sets already built, in the second equation above, to build new sets at a "powering stage" $\alpha + 1$ (identified by a successor ordinal).

We also note that at a "collecting stage" $\alpha$, identified by a limit ordinal, we collect together all objects previously constructed or "donated" that are scattered around in the various $V_N(\beta)$ for $\beta < \alpha$. Thus, ordinals serve as (formal) "stages" of set construction.

Comparing this formal definition with that in Section IV.2, we note that we deviate from the latter in that we include *all* subsets of $N \cup V_N(\alpha)$ at a powering stage, not only the "definable" (or "constructible") ones. □ ☡

**VI.6.3 Lemma ($V_N$ vs. $R_N$).** *For successor ordinals $\alpha$, $V_N(\alpha) = R_N(\alpha)$. For all other ordinals, $V_N(\alpha) = N \cup R_N(\alpha)$.*

*Proof.* A trivial induction: For $\alpha = 0$, $V_N(0) = N = N \cup R_N(0)$. For $\mathrm{Lim}(\alpha)$,

$$\begin{aligned} V_N(\alpha) &= \bigcup_{\beta<\alpha} V_N(\beta) \\ &= N \cup \bigcup_{\beta<\alpha} R_N(\beta) \qquad \text{since } V_N(\beta) \in \{R_N(\beta), N \cup R_N(\beta)\} \text{ by I.H.} \\ &= N \cup R_N(\alpha) \end{aligned}$$

For $\alpha = \beta + 1$,

$$\begin{aligned} V_N(\beta+1) &= \mathbf{P}(N \cup V_N(\beta)) \\ &= \mathbf{P}(N \cup R_N(\beta)) \qquad \text{by I.H.} \\ &= R_N(\beta+1) \end{aligned}$$

□

Thus, $N \cup \mathbf{WF}_N = \bigcup_{\alpha \in \mathrm{On}} V_N(\alpha)$. In $\mathbf{WF}_N$ we collect only the *sets* built from $N$, and leave "loose" urelements out of the collection. As in III.4.20, $\mathbb{V}_N$ will denote the class of *all sets* built from $N$. The question whether $\mathbf{WF}_N = \mathbb{V}_N$ is a subsidiary of the second claim made in VI.6.2, and will be settled shortly.

**VI.6.4 Proposition.** *$N \cup V_N(\alpha)$ is transitive for all $\alpha$.*

*Proof.* By induction on $\alpha$: $N \cup V_N(0) = N$ is transitive, for $x \in y \in N$ is refutable.

Consider $N \cup V_N(\alpha + 1)$, on the I.H. that $N \cup V_N(\alpha)$ is transitive. Let then $x \in y \in N \cup V_N(\alpha + 1)$; hence (why?) $x \in y \in V_N(\alpha + 1)$; therefore $x \in y \subseteq N \cup V_N(\alpha)$, so that $x \in N \cup V_N(\alpha)$. If $x \in N$, then $x \in N \cup V_N(\alpha + 1)$ and we are done, otherwise, $x \subseteq N \cup V_N(\alpha)$ by I.H. and hence $x \in V_N(\alpha + 1)$.

Let finally $\mathrm{Lim}(\alpha)$, and (I.H.) assume that all $N \cup V_N(\beta)$ are transitive for $\beta < \alpha$. Suppose that $x \in y \in N \cup V_N(\alpha) = N \cup \bigcup_{\beta<\alpha} V_N(\beta)$. Thus,

$$x \in y \in \bigcup_{\beta<\alpha} V_N(\beta)$$

so that $x \in y \in V_N(\beta)$ for some $\beta < \alpha$. By I.H., $x \in N \cup V_N(\beta) \subseteq N \cup V_N(\alpha)$. □

It follows that $\bigcup_{\alpha \in \mathrm{On}} V_N(\alpha) = N \cup \mathbf{WF}_N$ is transitive as well. Note however that $\mathbf{WF}_N$ is not transitive (unless $N = \emptyset$), since for any urelement $p$, $p \in N \in R_N(1) \subseteq \mathbf{WF}_N$, yet $p \notin \mathbf{WF}_N$.

**VI.6.5 Corollary.** *If there are no urelements (i.e., $N = \emptyset$), then $R_N(\alpha) = V_N(\alpha)$ is transitive for all $\alpha$.*

**VI.6.6 Corollary.** $(\forall\alpha)(\forall\beta < \alpha)V_N(\beta) \subseteq N \cup V_N(\alpha)$.

*Proof.* We do induction on $\alpha$. For $\alpha = 0$ the statement is vacuously satisfied.

The case for $\alpha + 1$, on the I.H. that the claim holds for $\alpha$: Let us first consider $\beta = \alpha < \alpha + 1$. Take $x \in V_N(\alpha)$. If $x \in N$, then we are done; else $x \subseteq N \cup V_N(\alpha)$ by VI.6.4, whence $x \in V_N(\alpha + 1)$. Thus

$$V_N(\alpha) \subseteq N \cup V_N(\alpha + 1) \tag{1}$$

Let next $\beta < \alpha$. The I.H. yields $V_N(\beta) \subseteq N \cup V_N(\alpha)$; hence $V_N(\beta) \subseteq N \cup V_N(\alpha + 1)$ by (1).

The case Lim($\alpha$): Here already $V_N(\beta) \subseteq V_N(\alpha)$, even without the help of I.H. □

**VI.6.7 Corollary.** $(\forall\alpha)(\forall\beta < \alpha)V_N(\beta) \in V_N(\alpha)$.

*Proof.* Induction on $\alpha$. For $\alpha = 0$ the claim is vacuously satisfied.

For $\alpha + 1$, $V_N(\alpha + 1) = \mathbf{P}(N \cup V_N(\alpha))$; hence

$$V_N(\alpha) \in V_N(\alpha + 1) \tag{1}$$

If, in general, $\beta < \alpha + 1$, then it remains to consider $\beta < \alpha$. By I.H., $V_N(\beta) \in V_N(\alpha)$. By (1) and VI.6.4, $V_N(\beta) \in V_N(\alpha + 1)$.

The case Lim($\alpha$): Let $\beta < \alpha$, hence $\beta + 1 < \alpha$. Now $V_N(\beta + 1) \subseteq \bigcup_{\gamma<\alpha} V_N(\gamma) = V_N(\alpha)$; thus, by (1), $V_N(\beta) \in V_N(\alpha)$ (the I.H. was not needed here). □

**VI.6.8 Corollary.** $(\forall\alpha)\alpha \subseteq V_N(\alpha)$.

*Proof.* Induction on $\alpha$. For $\alpha = 0$ the claim is trivial.

For $\alpha + 1$, $V_N(\alpha + 1) = \mathbf{P}(N \cup V_N(\alpha)) \ni \alpha$, by I.H. By VI.6.4, $\alpha \subseteq N \cup V_N(\alpha + 1)$; hence $\alpha \subseteq V_N(\alpha + 1)$, since ordinals are *pure sets* (VI.5.21). All in all, $\alpha + 1 = \alpha \cup \{\alpha\} \subseteq V_N(\alpha + 1)$.

The case Lim($\alpha$): $\beta \subseteq V_N(\beta) \subseteq V_N(\alpha)$ for all $\beta < \alpha$, by I.H. Thus, $\alpha = \bigcup \alpha = \bigcup\{\beta : \beta < \alpha\} \subseteq V_N(\alpha)$, where the first = is justified in Exercise VI.13. □

**VI.6.9 Corollary.** $\beta \in V_N(\alpha)$ *iff* $\beta < \alpha$.

*Proof. If part.* $\beta \in \alpha \subseteq V_N(\alpha)$ (by VI.6.8) implies $\beta \in V_N(\alpha)$.

*Only-if part.* Induction on $\alpha$. For $\alpha = 0$ the claim is vacuously satisfied, because $\beta \in N$ is refutable.

For $\alpha + 1$: Let $\beta \in V_N(\alpha + 1)$. Thus

$$\beta \subseteq V_N(\alpha) \tag{1}$$

since ordinals are pure sets. Why should $\beta < \alpha + 1$, that is, $\beta \leq \alpha$, or $\beta \subseteq \alpha$? Well, let $\gamma \in \beta$. Thus $\gamma \in V_N(\alpha)$ by (1). By I.H., $\gamma \in \alpha$.

The case Lim($\alpha$): Let $\beta \in V_N(\alpha) = \bigcup\{V_N(\gamma) : \gamma < \alpha\}$. So $\beta \in V_N(\gamma)$ for some $\gamma < \alpha$; hence, by I.H., $\beta < \gamma$. Thus, $\beta < \alpha$. □

**VI.6.10 Corollary.** On $\subseteq \bigcup_{\alpha\in\mathrm{On}} V_N(\alpha)$.

**VI.6.11 Remark.** By VI.6.6 we have a *hierarchy* of sets $V_N(\alpha)$, in the sense that as the stages, $\alpha$, of the construction progress, we obtain more and more inclusive sets.

The hierarchy is *proper*, that is, $V_N(\beta) \subset N \cup V_N(\alpha)$ if $\beta < \alpha$, i.e., the construction keeps adding new stuff. This is because of $\beta \in V_N(\alpha) - V_N(\beta)$ (by VI.6.9). Alternatively, if $V_N(\beta) = N \cup V_N(\alpha)$ for some $\beta < \alpha$, then, by VI.6.7, $V_N(\beta) \in V_N(\beta)$. □

At the end of all this, have we got enough sets to "do set theory"? In other words, are all the axioms of set theory true in the "real"

$$\bigcup_{\alpha\in\mathrm{On}} V_N(\alpha) \tag{$A$}$$

or, formally, are the axioms provable when *relativized* to $\bigcup_{\alpha\in\mathrm{On}} V_N(\alpha)$ (cf. Section I.7)? And are these *all* the sets we can get if we start with a set $N$ of atoms? That is, is it the case that

$$\mathbb{U}_N = \bigcup_{\alpha\in\mathrm{On}} V_N(\alpha) \tag{$B$}$$

Let us address these two questions in order. First a lemma.

**VI.6.12 Lemma.** *For any set $x$, $x \subseteq N \cup \mathbf{WF}_N$ implies $x \in N \cup \mathbf{WF}_N$.*

*Proof.* If $x = \emptyset$, then $x \in V_N(1)$. So assume that $x \neq \emptyset$, and let $\alpha_y$ denote, for each $y \in x$, the smallest $\alpha$ such that $y \in V_N(\alpha)$. By collection, $S = \{\alpha_y : y \in x\}$ is a set; hence, $\sup S$ exists (by VI.5.22). Say it is $\beta$. But then (by VI.6.6), $x \subseteq N \cup V_N(\beta)$; hence $x \in V_N(\beta + 1)$. □

**VI.6.13 Theorem.** *For any initial set of urelements $N$, the class $N \cup \mathbf{WF}_N = \bigcup_{\alpha\in\mathrm{On}} V_N(\alpha)$ satisfies all the axioms of set theory, that is,*

$$\mathfrak{J} = (L_{\mathrm{Set}}, \mathrm{ZFC}, N \cup \mathbf{WF}_N)$$

*is a formal model of ZFC.*

We are somewhat simplifying the notation in our applications of the material of Section I.7. Thus, we have omitted the last component, "$\mathscr{T}$", in "$\mathfrak{J} = (L_{\mathrm{Set}}, \mathrm{ZFC}, N \cup \mathbf{WF}_N)$". If we ever need to write "$P^{\mathscr{T}}$" (for some predicate $P$), we will write "$P^{N\cup\mathbf{WF}_N}$" instead. Two more simplifications in our notation are:

(1) We wrote $L_{\text{Set}}$, but we mean here the basic language *augmented* by the various defined symbols we have introduced to this point.
(2) We wrote $N \cup \mathbf{WF}_N$ rather than "$\mathscr{M}(x)$", where the latter is the defining formula of the class term.

*Proof.* The reader may wish to review the concepts in Section I.7.

Now, the requirement that

$$\vdash_{\text{ZFC}} (\exists x)(x \in N \cup \mathbf{WF}_N)$$

is trivially met by $\vdash_{\text{ZFC}} 0 \in N \cup \mathbf{WF}_N$ (cf. VI.6.10) and the substitution axiom.

We interpret now our two nonlogical symbols, $U$ and $\in$. We interpret both as "themselves". That is, $\in^{N\cup\mathbf{WF}_N} \equiv \in$ and $U^{N\cup\mathbf{WF}_N} \equiv U$.

A moment's reflection (cf. I.7.4) shows that $U(x)$ is "true in $N \cup \mathbf{WF}_N$"[†] iff $x \in N$. Indeed, $\models_{\mathfrak{I}} U(x)$ is short for

$$\vdash_{\text{ZFC}} x \in N \cup \mathbf{WF}_N \rightarrow U(x)$$

Thus $x \in \mathbf{WF}_N$ is untenable. Therefore $x \in N$. The other direction is trivial. Correspondingly, "$A$ is a set" translates to "$A$ is a set *and* $A \in N \cup \mathbf{WF}_N$."

Next, to facilitate the argument that follows, we look at the (defined) symbol "$\subseteq$": Suppose that $A$, $B$ are in $N \cup \mathbf{WF}_N$. What will the interpretation of $A \subseteq B$, that is, of

$$(\forall x)(x \in A \rightarrow x \in B) \tag{1}$$

be? It will be

$$(\forall x \in N \cup \mathbf{WF}_N)(x \in A \rightarrow x \in B) \tag{2}$$

Trivially, (1) implies (2). Interestingly, (2) implies (1): Indeed, to prove (1) (from (2)), let $x \in A$. Since also $A \in N \cup \mathbf{WF}_N$, we get $x \in N \cup \mathbf{WF}_N$ by transitivity of $N \cup \mathbf{WF}_N$. Then $x \in B$ by (2).

Thus, Platonistically, $\subseteq$ has the same meaning in $N \cup \mathbf{WF}_N$ as in the whole universe $\mathbb{U}_N$.

[†] It is easier expositionally to refer to $N \cup \mathbf{WF}_N$, meaning really $\mathfrak{I}$. The jargon "true in" was introduced (with apologies) on p. 80.

We now turn to the verification of all the axioms in $N \cup \mathbf{WF}_N$.

(i) *The axiom* $(\exists x)(\forall y)(U(y) \leftrightarrow y \in x)$ translates to

$$(\exists x \in N \cup \mathbf{WF}_N)(\forall y \in N \cup \mathbf{WF}_N)(U(y) \leftrightarrow y \in x)$$

Since $N \in N \cup \mathbf{WF}_N$ is provable (e.g., I.6.7), to prove the above it suffices to argue the case for

$$(\forall y \in N \cup \mathbf{WF}_N)(U(y) \leftrightarrow y \in N)$$

But this we have already done.

(ii) That *the axiom* $U(x) \rightarrow (\forall y) y \notin x$ is "true in $N \cup \mathbf{WF}_N$" means

$$\vdash_{\mathrm{ZFC}} x \in N \cup \mathbf{WF}_N \rightarrow U(x) \rightarrow (\forall y \in N \cup \mathbf{WF}_N) y \notin x$$

which is a tautological consequence of $U(x) \rightarrow (\forall y \in N \cup \mathbf{WF}_N) y \notin x$, and the latter trivially follows in ZFC from $U(x) \rightarrow y \in N \cup \mathbf{WF}_N \rightarrow y \notin x$, itself a tautological consequence of $U(x) \rightarrow y \notin x$.[†]

(iii) *Axiom of extensionality*. It says that for any sets $A$ and $B$,

$$A \subseteq B \wedge B \subseteq A \rightarrow A = B$$

Now, for any sets $A$, $B$ in $N \cup \mathbf{WF}_N$, the relativization of this is provable in ZFC, since "=" is logical, and we saw above (the equivalence of (1) and (2)) that "$\subseteq$" relativizes over $N \cup \mathbf{WF}_N$ as itself.

(iv) *Axiom of separation*. It says that for any set $B$ and class $\mathbb{A}$, $\mathbb{A} \subseteq B$ implies that $\mathbb{A}$ is a set. To see why this is true in $N \cup \mathbf{WF}_N$,[‡] let $B \in N \cup \mathbf{WF}_N$ and $\mathbb{A} \subseteq B$. Thus, in ZFC, $\mathbb{A}$ *is* a set (recall the invariance of meaning of "$\subseteq$"). To prove that $(\mathbb{A} \text{ is a set})^{N \cup \mathbf{WF}_N}$, equipped with our preliminary remarks at the onset of the proof, we only need to show that $\mathbb{A} \in N \cup \mathbf{WF}_N$. Now, $B \in V_N(\alpha)$ for some $\alpha$; hence (VI.6.4), $\mathbb{A} \subseteq B \subseteq N \cup V_N(\alpha)$. Therefore, $\mathbb{A} \in V_N(\alpha + 1)$; hence $\mathbb{A} \in N \cup \mathbf{WF}_N$.

(v) *Axiom of pairing*. For any $a, b$ in $N \cup \mathbf{WF}_N$ one must find a set $C \in N \cup \mathbf{WF}_N$ such that $a \in C$ and $b \in C$. We can take $C = \{a, b\}$, since $a \in V_N(\alpha)$ and $b \in V_N(\beta)$ implies (using VI.6.6) that $\{a, b\} \in V_N(\max(\alpha, \beta) + 1)$.

(vi) *Axiom of union*. For any set $A \in N \cup \mathbf{WF}_N$ we need to show that there is a set $B \in N \cup \mathbf{WF}_N$ such that, for all sets $x$ in $N \cup \mathbf{WF}_N$,[§]

$$x \in A \rightarrow x \subseteq B$$

[†] $\vdash (\forall y)(\mathscr{A} \rightarrow \mathscr{B}) \leftrightarrow (\mathscr{A} \rightarrow (\forall y)\mathscr{B})$, provided $y$ is not free in $\mathscr{A}$.

[‡] Armed with I.7.4, the reader will not be confused by the frequent occurrence of the *argot* "is true in $N \cup \mathbf{WF}_N$" in this proof.

[§] Note that we have translated $\subseteq$ by itself, due to (1) and (2).

We can take $B = N \cup V_N(\alpha)$, where $A \in V_N(\alpha)$. Indeed, $x \in A$ implies $x \in N \cup V_N(\alpha)$ by VI.6.4; hence, $x$ being a set, $x \subseteq N \cup V_N(\alpha)$ by VI.6.4 again. Of course, $B \in N \cup \mathbf{WF}_N$.

(vii) *Power set axiom*. We need to show that for any set $A \in N \cup \mathbf{WF}_N$ there is a set $B \in N \cup \mathbf{WF}_N$ such that, for all $x \in N \cup \mathbf{WF}_N$,

$$x \subseteq A \rightarrow x \in B.$$

We can take $B = V_N(\alpha + 1)$, where $A \in V_N(\alpha)$, since $A \subseteq N \cup V_N(\alpha)$ by VI.6.4.

(viii) *Collection*. We need to show the truth of

$$(\forall x \in A)(\exists y)\mathscr{F}[x, y] \rightarrow (\exists z)(\forall x \in A)(\exists y \in z)\mathscr{F}[x, y]$$

in $N \cup \mathbf{WF}_N$, that is, for any $A$ and formula $\mathscr{F}$,

$$A \in N \cup \mathbf{WF}_N \quad \text{and} \quad (\forall x \in A)(\exists y \in N \cup \mathbf{WF}_N)\mathscr{F}[x, y] \tag{3}$$

*imply within ZFC* that there is a set[†] $z$ in $N \cup \mathbf{WF}_N$ such that

$$(\forall x \in A)(\exists y \in z)\mathscr{F}[x, y] \tag{4}$$

So assume (3). This we view as $(\forall x \in A)(\exists y)\mathscr{G}[x, y]$, where $\mathscr{G}[x, y]$ is "$y \in N \cup \mathbf{WF}_N \wedge \mathscr{F}[x, y]$". We can now apply collection (in ZFC) to obtain a set $B$ (in ZFC) such that

$$(\forall x \in A)(\exists y \in B)\mathscr{G}[x, y]$$

or

$$(\forall x \in A)(\exists y \in B)(y \in N \cup \mathbf{WF}_N \wedge \mathscr{F}[x, y]) \tag{5}$$

By (5) and Lemma VI.6.12, $z = B \cap (N \cup \mathbf{WF}_N)$ is what we want for (4).

(ix) *Axiom of infinity*. We need an inductive set in $N \cup \mathbf{WF}_N$. Since $\omega \in N \cup \mathbf{WF}_N$ by VI.6.10, we are done.

(x) *AC*. Let $S$ be a set of nonempty sets in $N \cup \mathbf{WF}_N$. By AC (in ZFC), there is a choice function, $f : S \rightarrow \bigcup S$, such that $f(x) \in x$ for all $x \in S$. We want to show that $f$ is in $N \cup \mathbf{WF}_N$. Now by (iv) and (vi), $\bigcup S \in N \cup \mathbf{WF}_N$; hence $S \times \bigcup S \in N \cup \mathbf{WF}_N$ using (iv), (vi), and (vii), since $S \times \bigcup S \subseteq \mathbf{P}(S \cup \mathbf{P}(S \cup \bigcup S))$. Thus, $f \subseteq S \times \bigcup S$ implies $f \in N \cup \mathbf{WF}_N$.

(xi) *Axiom of foundation*. We left this till the very end for a special reason. We will show that $N \cup \mathbf{WF}_N$ would satisfy foundation *even if we did*

[†] Cf. III.8.4.

*not include foundation in ZFC.*[†] Let then $\emptyset \neq \mathbb{A} \subseteq N \cup \mathbf{WF}_N$. Take $\alpha = \min\{\beta : \mathbb{A} \cap V_N(\beta) \neq \emptyset\}$, and pick an $A \in \mathbb{A} \cap V_N(\alpha)$ (auxiliary constant). If $A$ is an urelement, then

$$(\exists x \in \mathbb{A})(\forall y \in \mathbb{A})y \notin x$$

is provable, since

$$(\forall y \in \mathbb{A})y \notin A \tag{6}$$

is. If $A$ is a set, then (6) is still provable (in ZFC without foundation): First, $A \notin V_N(\gamma)$ if $\gamma < \alpha$. Thus, $\alpha = \delta + 1$ for some $\delta$ (why?); hence $A \subseteq N \cup V_N(\delta)$. Then, $y \in A$ implies $y \in N \cup V_N(\delta)$, so that $y \in V_N(\max(0, \delta))$; hence $y \notin \mathbb{A}$ (else $\alpha \leq \max(0, \delta)$). □

☡ Part (xi) in the proof above was carried out without foundation. Indeed, the whole theorem can be proved without foundation, in "ZFC − f" – where "f" stands for foundation. This is due to the feasibility of basing everything in the proof on the Kuratowski pairing, $\langle x, y\rangle = \{\{x\}, \{x, y\}\}$, while defining ordinals as in VI.4.25. Indeed, everything we have said up until now (except for the examples regarding the properties of the collapsing function) can be said without the benefit of foundation.

Thus, the whole construction has built more than we were willing to admit initially. We have built a formal model of ZFC in $\mathfrak{J}' = (L_{\mathrm{Set}}, \mathrm{ZFC} - \mathrm{f}, N \cup \mathbf{WF}_N)$ rather than in "just" $\mathfrak{J} = (L_{\mathrm{Set}}, \mathrm{ZFC}, N \cup \mathbf{WF}_N)$. I.7.10 yields at once: ☡

**VI.6.14 Corollary.** *If ZFC* without foundation *is consistent, then so is ZFC.*

☡ But we do have foundation – that is, its suspension was only temporary, to obtain VI.6.14. ☡

**VI.6.15 Theorem.** $\mathbb{U}_N = \bigcup_{\alpha \in \mathrm{On}} V_N(\alpha)$.

*Proof.* By $\mathbb{U}_N$ we understand, of course, $\{x : sp(x) \subseteq N\}$ (cf. VI.6.2). The $\supseteq$-part is trivial, so we address the $\subseteq$-part. Let us use $\in$-induction over $\mathbb{U}_N$, so let $x \in \mathbb{U}_N$, and assume (I.H.) that for all $y \in x$, $y \in N \cup \mathbf{WF}_N$. Thus, $x \subseteq N \cup \mathbf{WF}_N$. By VI.6.12, $x \in N \cup \mathbf{WF}_N$. □

**VI.6.16 Corollary.** $\mathbf{WF}_N = \mathbb{V}_N$.

[†] Once again we point out that there is no circularity in this assertion, for ordinals can be defined without the presence of foundation (see the discussion following VI.4.25). Another revision that one needs to make in this (*temporary*!) rewriting of our development is the definition of $\langle x, y\rangle$. To avoid foundation one defines $\langle x, y\rangle = \{\{x\}, \{x, y\}\}$.

**VI.6.17 Corollary.** *Foundation is equivalent to the statement* $\mathbb{V}_N = \mathbf{WF}_N$.

See also the discussion in II.1.4.

*Proof.* That foundation implies $\mathbb{V}_N = \mathbf{WF}_N$ was the content of the proof of VI.6.15. Conversely, if $\mathbb{V}_N = \mathbf{WF}_N$ holds, then foundation holds, since it is a theorem of ZFC − f in $\mathbf{WF}_N$. □

Another way to put all this is that *if we drop the foundation axiom*, then

$$\mathbf{WF}_N \subset \mathbb{V}_N$$

The sets in $\mathbb{V}_N - \mathbf{WF}_N$ are the *hypersets* (see Barwise and Moss (1991)).

We started off in Chapter II by proposing – after Russell – that sets be formed in stages. The concept of “stage” was necessarily vague there, yet it assisted us to choose a small group of “reasonable axioms” on which we based all our deductions hence. We have now come to a point that “stages” can be formalized within the theory!

**VI.6.18 Definition.** We say that a *set $x$ is formed from $N$ at stage*[†] $\alpha$ iff $x \in R_N(\alpha)$ (iff $x \in V_N(\alpha)$, since $x$ is a set).

Thus $R_N(\alpha)$ is the set of all sets formed at stage $\alpha$. □

Principle 0 of Chapter II says that “an arbitrary class is a set formed (from $N$) at some stage if all its members are formed (set-members) or given (urelement-members) at some earlier stage”, and Principle 1 says that “every set is constructed at some stage”. All this has now become *formally* true (with our final interpretation of what “stage” means).

Indeed, if the set $x$ is in $V_N(\alpha)$ and $\alpha$ is smallest (“earliest”), then $\alpha = \beta + 1$ (why?); hence $x \subseteq N \cup V_N(\beta) = N \cup R_N(\beta)$. That is, *all* the elements of $x$ are formed ($\in R_N(\beta)$) or given ($\in N$) at some *earlier* stage.

Conversely, if it is known for a *class* $\mathbb{A}$ that all $y \in \mathbb{A}$ satisfy $y \in V_N(\alpha_y)$, and if we are told that there is a stage *after* all the $\alpha_y$ (that is, $\sup\{\alpha_y : y \in \mathbb{A}\}$ exists and equals, say, $\beta$), then $\mathbb{A} \subseteq \bigcup_{y \in x} V_N(\alpha_y) \subseteq N \cup V_N(\beta)$ (the last $\subseteq$ by VI.6.6). Hence $\mathbb{A} \in V_N(\beta + 1)$, i.e., $\mathbb{A}$ is constructed at stage $\beta + 1$ from $N$, as a set. This formalizes Principle 2.

Principle 1 is formalized as VI.6.16.

[†] This is meant in the non-strict sense. $\alpha$ need not be the earliest stage (i.e., smallest ordinal) at which $x$ is formed.

**VI.6.19 Definition (Rank of an Object in $\mathbb{U}_N$).** The *rank* of an object $x$ in $\mathbb{U}_N$, $\rho_N(x)$, is the earliest stage $\alpha$ at which $x$ is formed from $N$, in the sense $\rho_N(x) = \min\{\alpha : x \in V_N(\alpha)\}$. □

**VI.6.20 Remark.** (1) We will normally suppress the subscript $N$ on $\rho$. See also VI.6.24 below.

(2) Definition VI.6.19 wants $\rho(x)$ to be the earliest stage $\alpha$ at which we can place the set or urelement $x$ as a *member* of $V_N(\alpha)$. This deviates from the standard definition given in most of the literature, where the rank is defined as the smallest $\alpha$ such that $x \subseteq V_N(\alpha)$.

We prefer VI.6.19 (the adoption of which affects computation of ranks, but no other theoretical results) because we find it aesthetically more pleasing not to have both sets and urelements at stage 0. The alternate definition gives rank 0 to $\emptyset$, as it does to any atom – see for example Barwise (1975). With respect to the literature that admits no urelements in the theory, our objection disappears.

(3) The adoption of VI.6.19 makes $\rho(x)$ a successor for all sets $x$. Indeed, if $\mathrm{Lim}(\rho(x))$ (why can it not be that $\rho(x) = 0$?), then, as $V_N(\rho(x)) = \bigcup\{V_N(\alpha) : \alpha < \rho(x)\}$, we would get $x \in V_N(\alpha)$ for some $\alpha < \rho(x)$.

(4) VI.6.19 yields $\rho(\alpha) = \alpha + 1$ (see below), while the standard rank, "$rk$", would have $rk(\alpha) = \alpha$ (Exercise VI.24). □

**VI.6.21 Proposition.** $(\forall\alpha)\rho(\alpha) = \alpha + 1$.

*Proof.* By VI.6.9, $\alpha \in V_N(\alpha + 1) - V_N(\beta)$, where $\beta \leq \alpha$. □

**VI.6.22 Example.** If $x \subseteq N$, where $N$ is a set of urelements, then $\rho_N(x) = 1$. Well, first, $x \notin N = V_N(0)$, and second, $x \in V_N(1) = \mathbf{P}(N \cup V_N(0))$.

In particular, $\rho_N(\emptyset) = 1$. □

**VI.6.23 Proposition.** *For any sets $x$, $y$,*

(*i*) *$x \in y$ implies $\rho(x) < \rho(y)$,*
(*ii*) *$x \subseteq y$ implies $\rho(x) \leq \rho(y)$.*

*Proof.* (*i*): Let $x \in y$ and $\rho(y) = \alpha + 1$. Then $x \in y \in \mathbf{P}(N \cup V_N(\alpha))$; hence $x \in N \cup V_N(\alpha)$, from which $\rho(x) \leq \max(0, \alpha)$.

(*ii*): Let $x \subseteq y$ and $\rho(y) = \alpha + 1$. Here, $x \subseteq N \cup V_N(\alpha)$; hence $x \in V_N(\alpha + 1)$; thus $\rho(x) \leq \alpha + 1$. □

**VI.6.24 Proposition.** *$\rho_N$ satisfies the recurrence equations*

$$\rho_N(x) = \begin{cases} 0 & \text{if } x \in N \\ \left(\bigcup_{y \in x} \rho_N(y)\right) + 1 & \text{otherwise} \end{cases}$$

*Proof.* $N = V_N(0)$ settles the first equation. Let now $x$ be a set and $\alpha = \bigcup_{y \in x} \rho_N(y)$, while $\rho_N(x) = \beta + 1$. Since $\rho_N(y) \le \alpha$ for all $y \in x$, we get $(\forall y \in x) y \in N \cup V_N(\alpha)$ (by VI.6.6); hence $x \subseteq N \cup V_N(\alpha)$; thus $x \in V_N(\alpha+1)$. This yields

$$\beta + 1 \le \alpha + 1 \tag{1}$$

By VI.6.23, $(\forall y \in x)\rho_N(y) < \beta + 1$; hence $(\forall y \in x)\rho_N(y) \le \beta$. Thus $\alpha \le \beta$; hence $\alpha + 1 \le \beta + 1$. Using (1), we get the second equation. □

The above recurrence shows that the dependence of $\rho_N$ on $N$ is straightforward (initialization), which justifies our lack of caution in suppressing the subscript $N$.

**VI.6.25 Example.** Let us re-compute $\rho(\emptyset)$: $\rho(\emptyset) = \left(\bigcup_{y \in \emptyset} \rho(y)\right) + 1 = 0 + 1 = 1$.

Next, let us compute again $\rho(x)$ for $\emptyset \ne x \subseteq N$ (where $N$ is our initial atom set): $\rho(x) = \left(\bigcup_{y \in x} \rho(y)\right) + 1 = (\bigcup\{0\}) + 1 = 0 + 1 = 1$. □

**VI.6.26 Example.** Let us rediscover the identity $\rho(\alpha) = \alpha + 1$, using induction over On in connection with VI.6.24. Use $\rho(\beta) = \beta + 1$ for $\beta < \alpha$ as I.H.

Then $\rho(\alpha) = \left(\bigcup_{\beta < \alpha} (\beta + 1)\right) + 1 = \sup^+(\alpha) + 1 = \alpha + 1$. □

**VI.6.27 Example.** Suppose that $f$ is a function with $\mathrm{dom}(f) \subseteq \omega + 1$, such that $f(\omega)\downarrow$. Let us estimate $f$'s rank. We know that $\langle \omega, x \rangle \in f$ for some $x$. Now,

$$\begin{aligned} \rho(\langle \omega, x \rangle) &= \rho(\{\omega, \{\omega, x\}\}) \\ &= \max(\omega + 1, \rho(\{\omega, x\})) + 1 \\ &= \max\left(\omega + 1, \max\left(\omega + 1, \rho(x)\right) + 1\right) + 1 \\ &\ge \omega + 3 \end{aligned}$$

By VI.6.23, $\rho(\langle \omega, x \rangle) < \rho(f)$; thus, $f \notin V_N(\omega + 3)$.

This entails, in particular, that an inhabitant of $V_N(\omega + 3)$ would be oblivious to the fact that there is a 1-1 correspondence $\omega \sim \omega + 1$, since even though $\omega$ and $\omega + 1$ are "visible" in $V_N(\omega + 3)$,[†] the 1-1 correspondence is not. □

[†] In anticipation of ordinal arithmetic in Section VI.10, we are taking here the notational liberty to write things such as "$\alpha + 3$" for $((\alpha + 1) + 1) + 1$.

**VI.6.28 Example.** Next, assume $\mathrm{Lim}(\alpha)$, and let $\beta < \gamma$, both in $V_N(\alpha)$, and $f : \gamma \to \beta$ be a 1-1 correspondence. Is $f \in V_N(\alpha)$?

$f \subseteq \gamma \times \beta$. Now,

$$\begin{aligned}\rho(\gamma \times \beta) &= \bigcup_{\langle\delta,\eta\rangle \in \gamma\times\beta} \rho(\langle\delta,\eta\rangle) + 1\\ &= \bigcup_{\langle\delta,\eta\rangle \in \gamma\times\beta} \max(\delta + 3, \eta + 3) + 1\\ &\le \gamma + 3, \qquad \text{since } \max(\delta + 3, \eta + 3) \le \gamma + 2\end{aligned}$$

Thus, $\rho(f) \le \gamma + 3$ by VI.6.23, so that $f \in V_N(\gamma + 3)$ and hence $f \in V_N(\alpha)$, since $\gamma + 3 < \alpha$. An inhabitant of $V_N(\alpha)$ *will* witness the fact that $\gamma \sim \beta$. □

What else is the rank function good for?

It allows us to formalize the argument in III.8.3(I) to prove that collection follows from the following restricted axiom (*replacement axiom*), and therefore it is equivalent to it. This result strengthens III.8.12 by proving the the last version ((1) below) implies the first (III.8.2) (see p. 173).

$$(\forall x \in A)(\exists! y)\mathscr{S}(x, y) \to (\exists z)(\forall x \in A)(\exists y \in z)\mathscr{S}(x, y) \tag{1}$$

To avoid repetitiousness in the arguments that follow, let us show once and for all that

**VI.6.29 Proposition.** (Tarski (1955).) *For every class* $\mathbb{B}$ *there is a* set $b \subseteq \mathbb{B}$ *such that*

(1) $\mathbb{B} \ne \emptyset \to b \ne \emptyset$,
(2) *b can be given as a set term in terms of* $\mathbb{B}$.

*Proof.* Let us define $b = \emptyset$ if $\mathbb{B} = \emptyset$. Otherwise, let us collect in $b$ all those members of $\mathbb{B}$ of least rank (compare with the idea developed in III.8.3(I)). That is,

$$b = \{x \in \mathbb{B} : (\forall y \in \mathbb{B})\rho(x) \le \rho(y)\} \tag{$i$}$$

By $(i)$, $b \subseteq \mathbb{B}$. By assumption on $\mathbb{B}$, there is a minimum $\alpha$ such that $\emptyset \ne \mathbb{B} \cap V_N(\alpha)$. Thus, $b \ne \emptyset$ and $(\forall x \in b)\rho(x) = \alpha$ (if some $x, y$ in $b$ have $\rho(x) < \rho(y)$, then, as $x, y$ are in $\mathbb{B}$ as well, we must also have $\rho(y) \le \rho(x)$, untenable). Thus, $b \subseteq V_N(\alpha)$; hence it is a set.

$(i)$ is the "computation" of $b$ as a set term in terms of $\mathbb{B}$. □

We now turn to show that "replacement" ((1) above) implies collection (there is no circularity in this, for anywhere that we have used collection, the restricted form (1) sufficed).

Assume then

$$(\forall x \in A)(\exists y)\mathscr{S}(x, y) \tag{2}$$

Thus, there is a *nonempty* class $\mathbb{B}_x = \{y : \mathscr{S}(x, y)\}$ for each $x \in A$.

Let, for each $x \in A$, $b_x \neq \emptyset$ be the set "computed" by VI.6.29($i$). Using class notation for readability, (2) translates into

$$(\forall x \in A)(\exists y)y \in \mathbb{B}_x \tag{2$'$}$$

We have by VI.6.29

$$(\forall x \in A)(\exists! y)y = b_x \tag{3}$$

Why "$\exists!$"? Because, referring to the proof of VI.6.29, there is only one minimum $\alpha$ such that $\mathbb{B}_x \cap V_N(\alpha) \neq \emptyset$, and hence only one $b_x$. On the other hand, $\vdash b_x = y \to b_x = z \to y = z$. By schema (1), (3) yields

$$(\exists z)(\forall x \in A)(\exists y \in z)y = b_x$$

Let then $C$ be a new constant, and add

$$(\forall x \in A)(\exists y)(y \in C \wedge y = b_x)$$

By the one point rule (I.6.2), the above implies $(\forall x \in A)b_x \in C$; thus $\{b_x : x \in A\}$ is a set by separation; hence so is $\bigcup\{b_x : x \in A\}$. Call this union $D$ (new constant).

We are almost done. Let $x \in A$. Then $\mathbb{B}_x \neq \emptyset$, hence by VI.6.29, $b_x \neq \emptyset$. This allows us to add a new constant $e$ and also add $e \in b_x$. By $b_x \subseteq D$ we have $e \in D$. By $b_x \subseteq \mathbb{B}_x$ we have $e \in \mathbb{B}_x$. Thus, $e \in D \wedge e \in \mathbb{B}_x$; hence

$$(\exists y \in D)y \in \mathbb{B}_x$$

By the deduction theorem $x \in A \to (\exists y \in D)y \in \mathbb{B}_x$; hence (generalizing)

$$(\forall x \in A)(\exists y \in D)y \in \mathbb{B}_x$$

from which, eliminating class notation,

$$(\exists z)(\forall x \in A)(\exists y \in z)\mathscr{S}(x, y)$$

This, along with (2), proves collection (III.8.2).

**VI.6.30 Example.** Let the relation $\mathbb{P}$ satisfy a "weak" MC, namely, for every nonempty *set* $x$, there is a $\mathbb{P}$-minimal element $y \in x$, i.e., $\neg(\exists z \in x)z \mathbin{\mathbb{P}} y$, or

$$\mathbb{P}\langle y\rangle \cap x = \emptyset$$

It will follow that $\mathbb{P}$ has "ordinary" (strong) MC, as defined in VI.1.22.

Indeed, let $\emptyset \neq \mathbb{A}$, and let $\mathbb{A}$ have no $\mathbb{P}$-minimal elements, that is,

$$\text{for all } a \in \mathbb{A}, \quad \mathbb{B}_a = \mathbb{P}\langle a\rangle \cap \mathbb{A} \neq \emptyset \tag{1}$$

Now, we have no reason to assume that the $\mathbb{B}_a$'s are sets (e.g., $\mathbb{P}$ might fail to be left-narrow). However, by VI.6.29, we get for each $a \in \mathbb{A}$ a *nonempty set* $b_a \subseteq \mathbb{B}_a$. Let

$$\mathbb{S} = \bigcup_{a \in \mathbb{A}} \big(\{a\} \times b_a\big)$$

Since $\mathbb{S} \subseteq \mathbb{P}$, $\mathbb{S}$ has "weak" MC as well (compare with Exercise VI.1), and it is left-narrow, since for all $a \in \mathrm{dom}(\mathbb{S})$ we have $\mathbb{S}\langle a\rangle = b_a$. By Exercise VI.4, there is an $a \in \mathbb{A}$ such that

$$\mathbb{S}\langle a\rangle \cap \mathbb{A} = \emptyset$$

or

$$b_a \cap \mathbb{A} = \emptyset$$

which contradicts (1).

In particular, taking $\mathbb{P} \equiv \in$ (the relation "$\in$"), this shows that the "set version" (single axiom) of foundation,

$$(\exists x \in y) \to (\exists x \in y)\neg(\exists z \in y) z \in x$$

is equivalent to the "class version" that we gave as a schema (III.7.2).

As promised in Remark VI.2.14, Corollary VI.2.13 can now be strengthened to allow $A$ to be any class, possibly proper. The restriction to a *set* $A$ in the proof of VI.2.13 was meant to allow the use of AC, proving there that well-foundedness implies MC. Now let $\mathbb{P}$ be well-founded over a *class* $\mathbb{A}$. The proof of VI.2.13, unchanged, now starting with "... let $\emptyset \neq B \subseteq \mathbb{A}$, *where $B$ is a set*,[†] ...", shows that $\mathbb{P}$ has *weak* MC over $\mathbb{A}$. In view of the equivalence of the strong and weak versions of MC, $\mathbb{P}$ has (strong) MC over $\mathbb{A}$. □

## VI.7. A Pairing Function on the Ordinals

In this section we establish a useful technical result that we will employ in Section VI.9 and in the next chapter. We show that On × On can be well-ordered, and when this is done,

$$\mathrm{On} \times \mathrm{On} \cong \mathrm{On}$$

[†] The italicised hypothesis is explicitly added since $\mathbb{A}$ may be proper class.

We start by noting that, since for any two ordinals $\alpha$, $\beta$ one has either $\alpha \le \beta$ or $\beta < \alpha$, it makes sense to define

$$\max(\alpha, \beta) = \begin{cases} \alpha & \text{if } \beta \le \alpha \\ \beta & \text{otherwise} \end{cases}$$

and

$$\min(\alpha, \beta) = \begin{cases} \alpha & \text{if } \alpha \le \beta \\ \beta & \text{otherwise} \end{cases}$$

Since $\le$ is $\subseteq$, we have $\max(\alpha, \beta) = \alpha \cup \beta$ and $\min(\alpha, \beta) = \alpha \cap \beta$.

**VI.7.1 Definition.** We define a relation $\lhd$ on On × On by

$$\begin{aligned} \langle \sigma, \tau \rangle \lhd \langle \alpha, \beta \rangle \quad \text{iff} \quad & \max(\sigma, \tau) < \max(\alpha, \beta) \vee \\ & \max(\sigma, \tau) = \max(\alpha, \beta) \wedge \\ & \big(\sigma < \alpha \vee (\sigma = \alpha \wedge \tau < \beta)\big) \end{aligned} \qquad \square$$

**VI.7.2 Proposition.** $\lhd$ *is a well-ordering on* On × On.

*Proof.* We delegate the details, for example that $\lhd$ is a linear order, to the reader (Exercise VI.26).

Let us argue that it has MC. To this end, let $\emptyset \neq \mathbb{A} \subseteq \mathrm{On} \times \mathrm{On}$. The class $\{\alpha \cup \beta : \langle \alpha, \beta \rangle \in \mathbb{A}\}$ has a smallest member $\gamma$. This is realized as $\gamma = \alpha \cup \beta$ for some (perhaps several) $\langle \alpha, \beta \rangle \in \mathbb{A}$. Among those, pick all with the smallest $\alpha$ (first component), i.e., setting

$$\mathscr{F}(\sigma, \tau) \overset{\text{def}}{\equiv} \gamma = \sigma \cup \tau \wedge \langle \sigma, \tau \rangle \in \mathbb{A}$$

form the class

$$\{\langle \alpha, \beta \rangle : \mathscr{F}(\alpha, \beta) \wedge (\forall \sigma)(\forall \tau)(\mathscr{F}(\sigma, \tau) \to \alpha \le \sigma)\} \tag{1}$$

and finally pick in (1) that $\langle \alpha, \beta \rangle$ with the smallest $\beta$.

Let us verify that $\langle \alpha, \beta \rangle$ is $\lhd$-minimal in $\mathbb{A}$: If $\langle \sigma, \tau \rangle \lhd \langle \alpha, \beta \rangle$ because $\sigma \cup \tau < \alpha \cup \beta = \gamma$, then $\langle \sigma, \tau \rangle \notin \mathbb{A}$ by the choice of $\gamma$. Let it then be so because $\sigma \cup \tau = \alpha \cup \beta = \gamma$, but $\sigma < \alpha$. Then $\langle \sigma, \tau \rangle \notin \mathbb{A}$ by the choice of $\alpha$. The last case to consider also yields $\langle \sigma, \tau \rangle \notin \mathbb{A}$, by the choice of $\beta$. □

**VI.7.3 Theorem.** $(\mathrm{On}^2, \lhd) \cong (\mathrm{On}, <)$.

*Proof.* By VI.7.2 and VI.3.20 we have *one* of

(1) $(\mathrm{On}^2, \lhd) \cong (< \langle \alpha \rangle, <)$ for some $\alpha$,

(2) $(\lhd\big\langle\langle\alpha,\beta\rangle\big\rangle, \lhd) \cong (\mathrm{On}, <)$,
(3) $(\mathrm{On}^2, \lhd) \cong (\mathrm{On}, <)$.

To the left of $\cong$ in (1) we have a proper class (e.g., $\mathrm{dom}(\mathrm{On}^2) = \mathrm{On}$). Thus, this case is untenable. Case (2) is impossible as well, for the left hand side of $\cong$ is a subclass of $\gamma \times \gamma$, where $\gamma = (\alpha \cup \beta) + 1$, and hence a set.

This leaves (3) as the only possibility. □

As a result, $\lhd$ is left-narrow on $\mathrm{On}^2$.

**VI.7.4 Remark.** The unique function $J : \mathrm{On}^2 \to \mathrm{On}$ that effects the isomorphism of Theorem VI.7.3 is an instance of a *pairing function* on the ordinals – that is, a 1-1, *total* function $\mathrm{On}^2 \to \mathrm{On}$. This particular one is also *onto*; thus there is an inverse $J^{-1} : \mathrm{On} \to \mathrm{On}^2$. We reserve the letters $K, L$ to write $J^{-1} = \langle K, L\rangle$. The $K, L$ are the first and second *projections* of $J$ and satisfy $\langle K, L\rangle \circ J = \mathbf{1}_{\mathrm{On}^2}$ and $J \circ \langle K, L\rangle = \mathbf{1}_{\mathrm{On}}$ (the latter only because $J$ is onto). Thus,

$$K(J(\alpha, \beta)) = \alpha$$

and

$$L(J(\alpha, \beta)) = \alpha$$

for all $\alpha, \beta$.

With the aid of $K, L$ we can enumerate all the pairs in $\mathrm{On}^2$ by the (total) function $\alpha \mapsto \langle K(\alpha), L(\alpha)\rangle$ on On. Note how each of $K$ and $L$ enumerates each ordinal $\sigma$ infinitely often (why?)

Pairing functions play an important role in recursion theory (from where the notation is borrowed here). For a detailed account of computable pairing functions on $\mathbb{N}$ see Tourlakis (1984). □

What are pairing functions good for? Section VI.9 will exhibit a substantial application. The next one will be given in Chapter VII. For now let us extend the coding of pairs (of ordinals) that $J$ effects into a coding of "vectors" of ordinals (compare with III.10.4).

**VI.7.5 Definition.** We define by induction on $n \in \omega$ the functions $J_n$:

$$\begin{aligned} J_1(\alpha) &= \alpha && \text{for all } \alpha \\ J_{n+1}(\vec{\alpha}_{n+1}) &= J(J_n(\vec{\alpha}_n), \alpha_{n+1}) && \text{for all } \vec{\alpha}_{n+1} \end{aligned}$$

where $\vec{\alpha}_n$ stands for the sequence $\alpha_1, \ldots, \alpha_n$.

We also define for each $n \in \omega$ the functions $\pi_i^n$ for[†] $i = 1, \ldots, n$ by

$$\begin{aligned} \pi_1^1(\alpha) &= \alpha && \text{for all } \alpha \\ \pi_{n+1}^{n+1}(\alpha) &= L(\alpha) && \text{for all } \alpha \\ \pi_i^{n+1}(\alpha) &= \pi_i^n\big(K(\alpha)\big) && \text{for all } \alpha \end{aligned}$$ □

It is trivial to verify that for each $n \in \omega$, $J_n : \mathrm{On}^n \to \mathrm{On}$ is a 1-1 correspondence of which $\alpha \mapsto \langle \pi_1^n(\alpha), \ldots, \pi_n^n(\alpha) \rangle$ is the inverse.

**VI.7.6 Proposition.** *For each $\alpha$, $\beta$, $J(\alpha, \beta) \geq \alpha$ and $J(\alpha, \beta) \geq \beta$.*

*Proof.* Fix a $\beta$, and let $\sigma < \tau$.

*Case 1.* If $\tau \leq \beta$, then $\langle \sigma, \beta \rangle \lhd \langle \tau, \beta \rangle$; hence $J(\sigma, \beta) < J(\tau, \beta)$.
*Case 2.* If $\tau > \beta$, then $\sigma \cup \beta < \tau \cup \beta$, so that again $\langle \sigma, \beta \rangle \lhd \langle \tau, \beta \rangle$; thus also $J(\sigma, \beta) < J(\tau, \beta)$.

This amounts to $\lambda\alpha.J(\alpha, \beta)$ being order-preserving on On; hence the first required inequality follows from VI.3.15. The second inequality is proved similarly. □

**VI.7.7 Corollary.** *For each, $n$, $\alpha$, and $i \in n + 1 - \{0\}$, $\pi_i^n(\alpha) \leq \alpha$.*

$J$ and $\lhd$ have a number of additional interesting properties. We discuss one more here and delegate the others to the exercises section.

**VI.7.8 Example.** We show here that $J[\omega^2] = \omega$.

*Throughout this example, $\ldots^2$ stands for $\ldots \times \ldots$,* not *for ordinal multiplication or exponentiation (which have not been introduced yet anyway).*

Let $\langle n, m \rangle \in \omega^2$, where at least one of $n$ and $m$ is nonzero.

*Case 1.* $n = 0$. Then the immediate predecessor is $\langle m - 1, m - 1 \rangle$; hence $J(n, m) = J(m - 1, m - 1) + 1$.
*Case 2.* $0 < n < m$. Then the next pair down is $\langle n - 1, m \rangle$; hence $J(n, m) = J(n - 1, m) + 1$.
*Case 3.* $n > m = 0$. Then the next pair down is $\langle n - 1, n - 1 \rangle$; hence $J(n, m) = J(n - 1, n - 1) + 1$.
*Case 4.* $n > m > 0$. Then the next pair down is $\langle n, m - 1 \rangle$; hence $J(n, m) = J(n, m - 1) + 1$.

[†] $i \in n + 1 - \{0\}$, if you want to avoid "…".

Thus, for each $\langle n, m\rangle \in \omega^2$, $J(n, m)$ is a successor (or $0 = J(0, 0)$); therefore $J[\omega^2] \subseteq \omega$. Now $J[\omega^2] = J(0, \omega)$ (Exercises VI.28 and VI.29); hence $J[\omega^2] \supseteq \omega$, by VI.7.6. Thus $\omega$ is a fixed point of $\lambda\alpha.J[\alpha^2]$. □

## VI.8. Absoluteness

We expand here on the notions introduced in Section I.7. We will be interested in exploring the phenomenon where inhabitants of universes $\mathbb{M}$, possibly much smaller than $\mathbb{U}_M$, can correctly tell that a sentence $\mathscr{A}$ is true in $\mathbb{U}_M$, even though their knowledge goes no further than what is going on in their "world" $\mathbb{M}$.

We start by repeating the definition of relativization of formulas, this time in the specific context of $L_{\text{Set}}$. Since we here use $L_{\text{Set}}$ as our interpretation language, we go one step further and interpret $\in$ as $\in$ and $U$ as $U$. Thus, we restate below Definition I.7.3 under these assumptions.

**VI.8.1 Definition (Relativization of Formulas and Terms).** Given a class $\mathbb{M}$ for which $\mathbb{M} \neq \emptyset$ is a theorem[†] and a formula $\mathscr{F}$. We denote by $\mathscr{F}^{\mathbb{M}}$ the formula obtained from $\mathscr{F}$ by replacing each occurrence of $(\exists x)$ in it by $(\exists x \in \mathbb{M})$.

More precisely, by induction on formulas we define

$$\begin{aligned} U^{\mathbb{M}}(x) &\equiv U(x) \\ (x \in y)^{\mathbb{M}} &\equiv x \in y \\ (x = y)^{\mathbb{M}} &\equiv x = y \\ (\neg\mathscr{A})^{\mathbb{M}} &\equiv (\neg(\mathscr{A}^{\mathbb{M}})) \\ (\mathscr{A} \vee \mathscr{B})^{\mathbb{M}} &\equiv (\mathscr{A}^{\mathbb{M}} \vee \mathscr{B}^{\mathbb{M}}) \\ \big((\exists x)\mathscr{A}\big)^{\mathbb{M}} &\equiv \big((\exists x \in \mathbb{M})\mathscr{A}^{\mathbb{M}}\big) \end{aligned}$$

Now let $\mathbb{T}(\vec{u}) = \{x : \mathscr{T}(x, \vec{u})\}$ be a class term depending on the (free) variables $\vec{u}$. Its relativization to a class $\mathbb{M}$ is defined as $\mathbb{T}^{\mathbb{M}}(\vec{u}) = \{x \in \mathbb{M} : \mathscr{T}^{\mathbb{M}}(x, \vec{u})\}$.

The terminology "$\mathbb{T}(\vec{u})$ is defined in $\mathbb{M}$" is *argot* for the assertion "$\mathbb{T}^{\mathbb{M}}(\vec{u}) \in \mathbb{M}$ is provable on the assumptions $u_i \in \mathbb{M}$ (for all $i$)". $\mathbb{M}$ is $\mathbb{T}$-*closed* iff $\mathbb{T}(\vec{u}) \in \mathbb{M}$ for all $u_i \in \mathbb{M}$. □

The reader must have noticed that we now use $\mathscr{F}^{\mathbb{M}}$ rather than $\mathscr{F}^{\mathscr{M}(x)}$ (cf. I.7.3), as that is the normal practice in the context of set theory.

Recall that the primary logical connectives are $\neg$, $\vee$, and $\exists$. In contrast, $\forall$, $\wedge$, $\rightarrow$, $\leftrightarrow$ are defined symbols, which is why the above definition does not refer to them.

Clearly, if $\mathscr{F}$ is quantifier-free, then $\mathscr{F}^{\mathbb{M}}$ is $\mathscr{F}$.

[†] Of ZF or of ZFC or of whatever fragment "ZFC′" of ZFC we want to use in a formal interpretation $\mathfrak{J} = (L_{\text{Set}}, \text{ZFC}', \mathbb{M})$.

To say that $\mathbb{T}(\vec{u})$ is defined in $\mathbb{M}$ is to say that for all $u_i \in \mathbb{M}$, $\mathbb{T}^{\mathbb{M}}(\vec{u})$ *is a set, and a member of* $\mathbb{M}$. Clearly, $\mathbb{T}^{\mathbb{U}_N}(\vec{u}) = \mathbb{T}(\vec{u})$, and "$\mathbb{T}(\vec{u})$ is defined in $\mathbb{U}_N$" simply means that for all $u_i$, $\mathbb{T}(\vec{u})$ is a set.

**VI.8.2 Example.** What is $\{a, b\}^{\mathbb{M}}$? It is

$$\begin{aligned}\{x \in \mathbb{M} : (x = a \vee x = b)^{\mathbb{M}}\} &= \{x \in \mathbb{M} : x = a \vee x = b\}\\ &= \{a, b\} \cap \mathbb{M}\end{aligned}$$

This proves (in ZF − f, for example) that

$$x \in \mathbb{M} \to y \in \mathbb{M} \to \{x, y\}^{\mathbb{M}} = \{x, y\}$$

That is, for $a$ and $b$ chosen in $\mathbb{M}$, "$\{a, b\}$" has the same meaning in $\mathbb{M}$ as it has in $\mathbb{U}_N$.

If $\mathbb{M}$ is $\{a, b\}$-closed, then $\{a, b\}$ is defined in $\mathbb{M}$. □

**VI.8.3 Remark ("Truth" in $\mathbb{M}$).** We use the short *argot* "$\mathscr{F}(x_1, \ldots, x_n)$ is true in $\mathbb{M}$" for the longer *argot* "$\mathscr{F}(x_1, \ldots, x_n)$ is true in $\mathfrak{J} = (L_{\mathrm{Set}}, \mathrm{ZFC}', \mathbb{M})$". We will often write this assertion as

$$\models_{\mathbb{M}} \mathscr{F}(x_1, \ldots, x_n) \tag{1}$$

We will recall from I.7.4 the translation of the above *argot*, (1), where we use here "ZFC′" for some unspecified fragment of ZFC:

$$\vdash_{\mathrm{ZFC}'} x_1 \in \mathbb{M} \wedge x_2 \in \mathbb{M} \wedge \cdots \wedge x_n \in \mathbb{M} \to \mathscr{F}^{\mathbb{M}}(x_1, \ldots, x_n) \tag{2}$$

The part "$x_1 \in \mathbb{M} \wedge x_2 \in \mathbb{M} \wedge \cdots \wedge x_n \in \mathbb{M} \to$" in (2) is empty if $\mathscr{F}$ is a sentence.

Platonistically (semantically), "truth in $\mathbb{M}$" is just that; in the sense of I.5. Indeed, the notation (1) states such truth from the semantic viewpoint as well. In this and the next section however, our use of (1) is in the syntactic sense (2). □

**VI.8.4 Remark.** Thinking once again Platonistically (*semantically*), let us verify that for any formula $\mathscr{F}$ and all $a, b, \ldots$ in $\mathbb{M}$,

$$\models_{\mathbb{M}} \mathscr{F}[\![ a, b, \ldots ]\!] \quad \text{iff} \quad \models_{\mathbb{U}_N} \mathscr{F}^{\mathbb{M}}[\![ a, b, \ldots ]\!] \tag{1}$$

assuming that $N$ is the supply of atoms we have used to build the von Neumann universe. This is an easy induction on formulas, and the details are left to the reader. Here are some cases: For $\mathscr{F} \equiv U(x)$ we have, for $a \in \mathbb{M}$,

$$\models_{\mathbb{M}} U(x)[\![ a ]\!] \quad \text{iff} \quad \models_{\mathbb{U}_N} U(x)[\![ a ]\!] \quad \text{iff (cf. VI.8.1)} \quad \models_{\mathbb{U}_N} U^{\mathbb{M}}(x)[\![ a ]\!]$$

Say $\mathscr{F} \equiv \neg\mathscr{A}$. Then, for $a, \ldots$ in $\mathbb{M}$,

$$\models_{\mathbb{M}} (\neg\mathscr{A})\,[\![\, a, \ldots \,]\!]$$

iff

$$\not\models_{\mathbb{M}} \mathscr{A}\,[\![\, a, \ldots \,]\!]$$

iff (by I.H.)

$$\not\models_{\mathbb{U}_N} \mathscr{A}^{\mathbb{M}}\,[\![\, a, \ldots \,]\!]$$

iff

$$\models_{\mathbb{U}_N} (\neg\mathscr{A})^{\mathbb{M}}\,[\![\, a, \ldots \,]\!]$$

Say $\mathscr{F} \equiv (\exists x)\mathscr{A}$. Then, for $a, \ldots$ in $\mathbb{M}$,

$$\models_{\mathbb{M}} \big((\exists x)\mathscr{A}\big)\,[\![\, a, \ldots \,]\!]$$

iff

$$(\exists i \in \mathbb{M}) \models_{\mathbb{M}} \mathscr{A}\,[\![\, i, a, \ldots \,]\!]$$

iff (by I.H.)

$$(\exists i \in \mathbb{M}) \models_{\mathbb{U}_N} \mathscr{A}^{\mathbb{M}}\,[\![\, i, a, \ldots \,]\!]$$

iff

$$(\exists i) \models_{\mathbb{U}_N} (i \in \mathbb{M} \wedge \mathscr{A}^{\mathbb{M}})\,[\![\, i, a, \ldots \,]\!]$$

iff

$$\models_{\mathbb{U}_N} (\exists x \in \mathbb{M})\mathscr{A}^{\mathbb{M}}\,[\![\, a, \ldots \,]\!]$$

iff

$$\models_{\mathbb{U}_N} \big((\exists x)\mathscr{A}\big)^{\mathbb{M}}\,[\![\, a, \ldots \,]\!]$$

Thus, there are two ways to semantically evaluate a formula $\mathscr{F}$ in $\mathbb{M}$. One is to act as an inhabitant of $\mathbb{M}$. You then evaluate $\mathscr{F}$ in the standard way indicated in I.5. The other way is to act as an inhabitant of $\mathbb{U}_N$. Before you evaluate $\mathscr{F}$ in $\mathbb{M}$, however, you ensure that it is *relativized* into $\mathscr{F}^{\mathbb{M}}$ and that the values you plug into free variables are from $\mathbb{M}$. Then, both methods yield the same result.

Note, nevertheless, that an inhabitant of $\mathbb{M}$ may *think* (because he evaluated so, and he knows of no worlds beyond his to know better) that a sentence $\mathscr{F}$ is true, when *in reality*, i.e., absolutely speaking, something somewhat different is true: $\mathscr{F}^{\mathbb{M}}$.

Sometimes (for some $\mathscr{F}$ and some $\mathbb{M}$) the reality in $\mathbb{M}$ and the absolute reality coincide, and this is wonderful, for, in that case, what an inhabitant of $\mathbb{M}$ considers to be true is really true. We will explore this phenomenon shortly. □

**VI.8.5 Example (Informal).** Let $M = \{a, \{a\}, \{a, b\}\}$, where $a \neq b$ are urelements. Set $A = \{a\}$ and $B = \{a, b\}$. Clearly, $A \neq B$; hence also $(A \neq B)^M$.

Yet,

$$\big((\forall x)(x \in A \leftrightarrow x \in B)\big)^M$$

that is,

$$(\forall x \in M)(x \in A \leftrightarrow x \in B)$$

is (really) true. In short (see previous remark)

$$\models_M (\forall x)(x \in A \leftrightarrow x \in B)$$

Thus, $M$ does not satisfy extensionality.

It turns out that transitive classes do not have this flaw ($M$, of course, is not transitive). □

**VI.8.6 Definition ($\Delta_0$-formulas).** The set of the $\Delta_0$-formulas is the smallest subset of all formulas of $L_{\mathrm{Set}}$ that

(1) includes all the atomic formulas (of the types $x_i = x_j$, $U(x_i)$, $x_i \in x_j$), and
(2) is such that whenever the formulas $\mathscr{A}, \mathscr{B}$ are included, so are $(\neg\mathscr{A})$, $(\mathscr{A} \vee \mathscr{B})$, and $((\exists x_i \in x_j)\mathscr{A})$ for any variables $x_i, x_j$ ($x_i \not\equiv x_j$). □

The $\Delta_0$-formulas are also called *restricted* formulas, as quantification is always bounded by asking that the quantified variable belong to some set $x_j$.

Once more, we refer here only to the connectives $\neg$, $\vee$, $\exists$, since the others ($\forall$, $\wedge$, etc.) are expressible in terms of them. As always, when writing down formulas, whether these are restricted or not, we will only use just enough brackets to avoid ambiguities.

**VI.8.7 Lemma.** *If* $\mathbb{M}$ *is a transitive class and* $\mathscr{A}(x_1, \ldots, x_n)$ *is a* $\Delta_0$*-formula, then for all* $x_i \in \mathbb{M}$*,*

$$\mathscr{A}(\vec{x}_n) \leftrightarrow \mathscr{A}^{\mathbb{M}}(\vec{x}_n) \tag{1}$$

The above claim (1) is short for

$$\vdash_{\mathrm{ZF-f}} x_1 \in \mathbb{M} \wedge \cdots \wedge x_n \in \mathbb{M} \rightarrow \Big(\mathscr{A}(\vec{x}_n) \leftrightarrow \mathscr{A}^{\mathbb{M}}(\vec{x}_n)\Big)$$

*Proof.* Induction on $\Delta_0$-formulas:

*Basis.* The contention follows from VI.8.1 and VI.8.6.

Take as I.H. that (1) holds for $\mathscr{A}$ and $\mathscr{B}$. It is trivial that it holds for $\neg\mathscr{A}$ and $\mathscr{A} \vee \mathscr{B}$ as well. Let us then concentrate on $(\exists y \in z)\mathscr{A}(y, \vec{x}_n)$.

$\rightarrow$: Assume now $b \in \mathbb{M}$, $a_1 \in \mathbb{M}, \ldots, a_n \in \mathbb{M}$ (all these letters are free variables), and also add the assumption $(\exists y \in b)\mathscr{A}(y, \vec{a}_n)$, that is,

$(\exists y)\big(y \in b \wedge \mathscr{A}(y, \vec{a}_n)\big)$. This allows us to introduce the assumption

$$Y \in b \wedge \mathscr{A}(Y, \vec{a}_n)$$

where $Y$ is a new constant. Since $b \in \mathbb{M}$, it follows that $Y \in \mathbb{M}$ by transitivity. Thus, $Y \in \mathbb{M} \wedge Y \in b \wedge \mathscr{A}(Y, \vec{a}_n)$, from which the basis case and the I.H. yield (via the Leibniz rule)

$$Y \in \mathbb{M} \wedge (Y \in b)^{\mathbb{M}} \wedge \mathscr{A}^{\mathbb{M}}(Y, \vec{a}_n)$$

The substitution axiom yields

$$(\exists y \in \mathbb{M})\big((y \in b)^{\mathbb{M}} \wedge \mathscr{A}^{\mathbb{M}}(y, \vec{a}_n)\big) \tag{2}$$

Thus, using VI.8.1,

$$\big((\exists y \in b)\mathscr{A}(y, \vec{a}_n)\big)^{\mathbb{M}} \tag{3}$$

By the deduction theorem (omitting the $\vdash$-subscript),

$$\vdash b \in \mathbb{M} \to a_1 \in \mathbb{M} \to \cdots \to (\exists y \in b)\mathscr{A}(y, \vec{a}_n) \to \big((\exists y \in b)\mathscr{A}(y, \vec{a}_n)\big)^{\mathbb{M}} \tag{4}$$

$\leftarrow$: Conversely, let $b \in \mathbb{M}, a_1 \in \mathbb{M}, \ldots, a_n \in \mathbb{M}$ (all these letters are free variables), and also add the assumption (3). By VI.8.1 this yields (2). Hence (via the Leibniz rule, the basis part, and the I.H.), $(\exists y \in \mathbb{M})\big(y \in b \wedge \mathscr{A}(y, \vec{a}_n)\big)$, i.e.,

$$(\exists y)\big(y \in \mathbb{M} \wedge y \in b \wedge \mathscr{A}(y, \vec{a}_n)\big)$$

from which tautological implication along with $\exists$-monotonicity yields

$$(\exists y)\big(y \in b \wedge \mathscr{A}(y, \vec{a}_n)\big)$$

The deduction theorem does the rest. □

Thus, Platonistically, a $\Delta_0$-formula does not think that it is someone else if you give it more or less "interpretive freedom" (from a transitive $\mathbb{M}$ to $\mathbb{U}_N$ and back). Its "meaning" is, somehow, "absolute".

Less well-endowed formulas could suffer a change in meaning as we go beyond a transitive class $\mathbb{M}$. For example, $(\forall x)\mathscr{B}(x)$ can be true if the search $(\forall x)$ is restricted to $\mathbb{M}$, but might fail to be so if the search is extended beyond $\mathbb{M}$. Similarly, a formula $(\exists x)\mathscr{B}(x)$ might be true in $\mathbb{U}_N$, for there we can find an $x$ that works (a "witness"), whereas in a "smaller" class $\mathbb{M}$ such an $x$ might fail to exist.

In view of Remark VI.8.4, we can read VI.8.7 also this way: If $\mathscr{F}$ is a $\Delta_0$-formula and $\mathbb{M}$ is transitive, then (Platonistically) for all $a, \ldots$ in $\mathbb{M}$,

$$\models_{\mathbb{M}} \mathscr{F}[\![a, \ldots]\!] \quad \text{iff} \quad \models_{\mathbb{U}_N} \mathscr{F}[\![a, \ldots]\!] \tag{5}$$

by (1) in VI.8.4. Thus, an inhabitant of $\mathbb{M}$ will think that a $\Delta_0$-sentence is true iff it is really true.

**VI.8.8 Definition (Absolute Formulas).** For formula $\mathscr{A}(\vec{x}_n)$ to be *absolute for a class* $\mathbb{M}$ (that is not necessarily transitive) means that

$$\vdash_{\mathrm{ZFC}'} x_1 \in \mathbb{M} \to \cdots \to x_n \in \mathbb{M} \to \big(\mathscr{A}(\vec{x}_n) \leftrightarrow \mathscr{A}^{\mathbb{M}}(\vec{x}_n)\big)$$

A class term $\mathbb{T}(\vec{x}_n)$ is *absolute for* $\mathbb{M}$ iff

$$\vdash_{\mathrm{ZFC}'} x_1 \in \mathbb{M} \to \cdots \to x_n \in \mathbb{M} \to \mathbb{T}(\vec{x}_n) = \mathbb{T}^{\mathbb{M}}(\vec{x}_n) \qquad \square$$

Thus, using the above terminology, VI.8.7 says that $\Delta_0$-formulas are absolute for *transitive* classes. Example VI.8.2 shows that (the term) $\{a, b\}$ is absolute for *any class* $\mathbb{M}$.

If $\mathbb{T}(\vec{u}) = \{x : \mathscr{T}(x, \vec{u})\}$ and $\mathscr{T}$ is absolute for $\mathbb{M}$, then for $u_i \in \mathbb{M}$,

$$\begin{aligned} \mathbb{T}^{\mathbb{M}}(\vec{u}) &= \{x \in \mathbb{M} : \mathscr{T}^{\mathbb{M}}(x, \vec{u})\} \\ &= \{x \in \mathbb{M} : \mathscr{T}(x, \vec{u})\} \qquad \text{by absoluteness of } \mathscr{T} \\ &= \mathbb{T}(\vec{u}) \cap \mathbb{M} \end{aligned}$$

If moreover we know that $\mathbb{T}(\vec{u}) \subseteq \mathbb{M}$ for all $u_i \in \mathbb{M}$, then $\mathbb{T}(\vec{u})$ is absolute for $\mathbb{M}$, as happened in the special case $\mathbb{T}(x, y) = \{x, y\}$.

In view of Definition VI.8.8, and inspecting the proof of VI.8.7, we can state at once:

**VI.8.9 Corollary.** *The set of formulas that are absolute for some class* $\mathbb{M}$ *is closed under the Boolean connectives and the bounded quantifiers* $(\exists x \in y)$ *and* $(\forall x \in y)$.

**VI.8.10 Corollary.** *Extensionality holds in any transitive class* $\mathbb{M}$.

*Proof.* Extensionality in $\mathbb{M}$ states that

$$\begin{aligned} &A \in \mathbb{M} \to B \in \mathbb{M} \to \\ &\qquad (\neg U(A) \wedge \neg U(B) \wedge (\forall x \in A) x \in B \wedge (\forall x \in B) x \in A \to A = B)^{\mathbb{M}} \end{aligned}$$

Since inside $(\ldots)^{\mathbb{M}}$ we have a $\Delta_0$-formula, the above is a tautological consequence of the extensionality axiom and VI.8.7. $\square$

**VI.8.11 Lemma.** *Foundation holds in any class* $\mathbb{M}$.

*Proof.* Let $\mathbb{M} = \{x : \mathscr{M}(x)\}$. Foundation says that

$$(\exists x).\mathscr{A}[x] \to (\exists x)(\mathscr{A}[x] \wedge \neg(\exists y \in x).\mathscr{A}[y]) \tag{1}$$

Its relativization to $\mathbb{M}$ is

$$(\exists x \in \mathbb{M}).\mathscr{A}^{\mathbb{M}}[x] \to (\exists x \in \mathbb{M})\big(\mathscr{A}^{\mathbb{M}}[x] \wedge \neg(\exists y \in \mathbb{M})(y \in x \wedge \mathscr{A}^{\mathbb{M}}[y])\big) \tag{2}$$

using VI.8.1. Letting now $a_1 \in \mathbb{M}, \ldots, a_n \in \mathbb{M}$, where $\vec{a}_n$ are the free variables in (2), we can have a proof of (2) in ZF, for it is an instance of the schema "$\in$ (the relation) has MC over $\mathbb{M}$", a provable schema by the foundation axiom (cf. VI.1.25). □

The lemma can be strengthened by effecting the interpretation in "ZF $-$ f", that is, dropping foundation. We have to take a few precautions:

(1) $\mathbb{M}$ is now not arbitrary, but is taken to be any subclass of $N \cup \mathbf{WF}_N$.
(2) $\langle x, y\rangle$ is defined by $\{\{x\}, \{x, y\}\}$ to avoid foundation.
(3) Ordinals are defined by VI.4.25.

We know then that we do have foundation in $N \cup \mathbf{WF}_N$ (provably) and can conclude the proof above in the same way, the only difference being the *reason* we have foundation (a theorem rather than an axiom).

**VI.8.12 Lemma.** *For any transitive class* $\mathbb{M}$ *and class term* $\mathbb{T}(\vec{u})$*,* $y = \mathbb{T}^{\mathbb{M}}(\vec{u})$ *iff* $(y = \mathbb{T}(\vec{u}))^{\mathbb{M}}$*, for all* $y, u_i \in \mathbb{M}$.

The proof can be carried out in ZF $-$ f. The statement is in the customary *argot*, but it states an implication, from *premises* $y \in \mathbb{M}$, $u_i \in \mathbb{M}$, to the *conclusion* $y = \mathbb{T}^{\mathbb{M}}(\vec{u}) \leftrightarrow (y = \mathbb{T}(\vec{u}))^{\mathbb{M}}$

*Proof.* We write throughout $\mathbb{T}(\vec{u}) = \{x : \mathscr{T}(x, \vec{u})\}$.

We calculate as follows:

$$\begin{aligned}
&\big(\neg U(y) \wedge \big(\forall z)(\mathscr{T}(z, \vec{u}) \leftrightarrow z \in y)\big)^{\mathbb{M}}\\
\leftrightarrow&\\
&\neg U(y) \wedge (\forall z \in \mathbb{M})(\mathscr{T}^{\mathbb{M}}(z, \vec{u}) \leftrightarrow z \in y)\\
\leftrightarrow&\\
&\neg U(y) \wedge (\forall z)\big(z \in \mathbb{M} \to (\mathscr{T}^{\mathbb{M}}(z, \vec{u}) \leftrightarrow z \in y)\big)\\
\leftrightarrow&\\
&\neg U(y) \wedge \big(\forall z)(z \in \mathbb{M} \wedge \mathscr{T}^{\mathbb{M}}(z, \vec{u}) \leftrightarrow z \in y\big)
\end{aligned}$$

The last equivalence above uses the Leibniz rule, the tautology

$$\big(\mathscr{A} \rightarrow (\mathscr{B} \leftrightarrow \mathscr{C})\big) \leftrightarrow (\mathscr{A} \wedge \mathscr{B} \rightarrow \mathscr{C}) \wedge (\mathscr{A} \wedge \mathscr{C} \rightarrow \mathscr{B})$$

and transitivity of $\mathbb{M}$ – which implies $z \in y \leftrightarrow z \in \mathbb{M} \wedge z \in y$. Noting (III.4.1) that the first line of our calculation says $(y = \mathbb{T}(\vec{u}))^{\mathbb{M}}$, while the last says $y = \mathbb{T}^{\mathbb{M}}(\vec{u})$; we are done. □

**VI.8.13 Remark.** The above result is useful: We often need to show that the $\mathbb{M}$-relativization of the formula "$\{x : \mathscr{A}(x, \vec{u})\}$ is a set" is provable. That is, we need to show, for $u_i \in \mathbb{M}$ (free variables), the derivability of

$$\big((\exists y) y = \mathbb{A}(\vec{u})\big)^{\mathbb{M}} \tag{1}$$

where we have set $\mathbb{A}(\vec{u}) = \{x : \mathscr{A}(x, \vec{u})\}$.

(1) stands for

$$(\exists y \in \mathbb{M})\big(y = \mathbb{A}(\vec{u})\big)^{\mathbb{M}}$$

which under the assumptions of VI.8.12 is provably equivalent to

$$(\exists y \in \mathbb{M}) y = \mathbb{A}^{\mathbb{M}}(\vec{u})$$

Thus, to prove (1), it is necessary and sufficient to prove that $\mathbb{A}$ is defined in $\mathbb{M}$.

One would apply this remark to proving that axioms such as those for separation, pairing, union, and power set hold in a transitive class. □

**VI.8.14 Corollary.** *Let $\mathbb{M}$ be transitive, $\mathbb{S}$ be absolute for $\mathbb{M}$, and $\mathbb{T}$ be absolute for* and *defined in $\mathbb{M}$. Assume also that the formula $\mathscr{F}$ is absolute for $\mathbb{M}$. Then:*

$(i)$ $\mathscr{F}[\mathbb{T}(\vec{u})]$ *is absolute for* $\mathbb{M}$.
$(ii)$ $\mathbb{S}[\mathbb{T}(\vec{u})]$ *is absolute for* $\mathbb{M}$.

*Proof.* Let $a_1 \in \mathbb{M}, \ldots,\ u_1 \in \mathbb{M}, \ldots,$ where $a_1, \ldots, u_1, \ldots$ are all the free variables occurring in the formulas above.

$(i)$: We first relativize $\mathscr{F}[\mathbb{T}(\vec{u})]$. This formula means (see III.11.16)

$$(\exists y)\big(\mathscr{F}[y] \wedge y = \mathbb{T}(\vec{u})\big) \tag{1}$$

Thus, $\big(\mathscr{F}[\mathbb{T}(\vec{u})]\big)^{\mathbb{M}}$ is provably equivalent to (using the absoluteness assumptions and Leibniz rule)

$$(\exists y \in \mathbb{M})\big(\mathscr{F}[y] \wedge (y = \mathbb{T}(\vec{u}))^{\mathbb{M}}\big) \tag{2}$$

By VI.8.12, (2) is provably equivalent to

$$(\exists y \in \mathbb{M})\big(\mathscr{F}[y] \wedge y = \mathbb{T}^{\mathbb{M}}(\vec{u})\big)$$

and hence to

$$(\exists y \in \mathbb{M})\big(\mathscr{F}[y] \wedge y = \mathbb{T}(\vec{u})\big) \tag{3}$$

since $\mathbb{T}$ is absolute for $\mathbb{M}$.

Now we want to argue that (3) is provably equivalent to (1): Indeed, (3) implies (1) trivially; conversely, (3) follows from (1), for if $y$ (auxiliary constant) works in the latter, then it satisfies $y = \mathbb{T}[\vec{u}]$; hence $y \in \mathbb{M}$ under the assumptions on $\mathbb{T}$ and $\vec{u}$.

$(ii)$: Next, start by observing that $\mathscr{S}$, where $\mathbb{S}(\vec{z}) = \{x : \mathscr{S}(x, \vec{z})\}$, is absolute for $\mathbb{M}$, since for $x, z_i \in \mathbb{M}$ (free variables), using "$\leftrightarrow$" conjunctionally, we have

$$\begin{aligned}
\mathscr{S}^{\mathbb{M}}(x, \vec{z}) &\leftrightarrow x \in \mathbb{S}^{\mathbb{M}}(\vec{z}) \\
&\leftrightarrow x \in \mathbb{S}(\vec{z}) \qquad \text{by absoluteness of } \mathbb{S} \\
&\leftrightarrow \mathscr{S}(x, \vec{z})
\end{aligned}$$

Thus,

$$\begin{aligned}
\big(\mathbb{S}[\mathbb{T}(\vec{u})]\big)^{\mathbb{M}} &= \Big\{x \in \mathbb{M} : \big(\mathscr{S}[x, \mathbb{T}(\vec{u})]\big)^{\mathbb{M}}\Big\} \\
&= \{x \in \mathbb{M} : \mathscr{S}[x, \mathbb{T}(\vec{u})]\}, \qquad \text{by part } (i)^{\dagger} \\
&= \mathbb{S}^{\mathbb{M}}[\mathbb{T}(\vec{u})] \\
&= \mathbb{S}[\mathbb{T}(\vec{u})], \qquad \text{by absoluteness of } \mathbb{S} \qquad \square
\end{aligned}$$

**VI.8.15 Example.** In particular, for any transitive class $\mathbb{M}$ that is $\{a, b\}$-closed, $\{a, \{a, b\}\}^{\mathbb{M}} = \{a, \{a, b\}\}$ and $\{\{a\}, \{a, b\}\}^{\mathbb{M}} = \{\{a\}, \{a, b\}\}$ are provable in ZF − f[‡] for $a \in \mathbb{M}$ and $b \in \mathbb{M}$. In other words, for such a class *either implementation* of the ordered pair $\langle a, b\rangle$ (among the two that we have mentioned) *is an absolute term.* □

**VI.8.16 Lemma.** *The following are absolute for any transitive class* $\mathbb{M}$*:*

$(i)$ $A \subseteq B$.
$(ii)$ $A = \emptyset$.
$(iii)$ *$A$ is a pair* (*also,* $A = \{x, y\}$).
$(iv)$ *$A$ is an ordered pair* (*also,* $A = \langle x, y\rangle$).

[†] Note that $\mathbb{T}(\vec{u}) \in \mathbb{M}$.

[‡] "f" enters in proving $\{a, \{a, b\}\} = \{a', \{a', b'\}\} \to a = a' \wedge b = b'$ and is not needed here.

$(v)$ $x = \pi(A)$ ($\pi(A)$ *is the first projection if* $A$ *is an ordered pair;* $\emptyset$ *otherwise*).

$(vi)$ $x = \delta(A)$ ($\delta(A)$ *is the second projection if* $A$ *is an ordered pair;* $\emptyset$ *otherwise*).

$(vii)$ *$A$ is a relation.*

$(viii)$ *$A$ is an order.*

$(ix)$ *$A$ is a function* (*also, $A$ is a* 1-1 *function*).

$(x)$ *$A$ is a transitive set.*

$(xi)$ *$A$ is an ordinal.*

$(xii)$ *$A$ is a limit ordinal.*

$(xiii)$ *$A$ is a successor.*

$(xiv)$ $A \in \omega$ (*or, $A$ is a natural number*).

$(xv)$ $A = \omega$.

$(xvi)$ $\{a, b\}$.

$(xvii)$ $\emptyset$.

$(xviii)$ $A - B$.

$(xix)$ $\bigcup A$.

$(xx)$ $\bigcap A$ *(to make this term total we re-define* $\bigcap \emptyset$ *as* $\emptyset$*).*

$(xxi)$ $x \in \mathrm{dom}(A)$.

$(xxii)$ $x \in \mathrm{ran}(A)$.

$(xxiii)$ $(*x \in \mathrm{dom}(A))\mathscr{F}$*, if* $\mathscr{F}$ *is absolute for* $\mathbb{M}$*, where "$*$" is* $\exists$ *or* $\forall$.

$(xxiv)$ $(*x \in \mathrm{ran}(A))\mathscr{F}$*, if* $\mathscr{F}$ *is absolute for* $\mathbb{M}$*, where "$*$" is* $\exists$ *or* $\forall$.

*Add the assumption that* $\mathbb{M}$ *is* $\{a, b\}$*-closed. Then the following terms are absolute for* $\mathbb{M}$*:*

(1) $A \times B$.

(2) $\mathrm{dom}(A)$.

(3) $\mathrm{ran}(A)$.

*Proof.* Most of these will be left to the reader (Exercise VI.61). Let us sample a few:

$(iii)$: $A$ is a pair: $(\exists x \in A)(\exists y \in A)(\forall z \in A)(z = x \vee z = y)$. This is a $\Delta_0$-formula, and hence absolute for any transitive class.

$(x)$: $A$ is a transitive set: $\neg U(A) \wedge (\forall y \in A)(\forall x \in y) x \in A$.

$(xiv)$: $A \in \omega$: "$A$ is an ordinal $\wedge$ $A$ is a successor or 0 $\wedge$ $(\forall x \in A)x$ is a successor or 0" is a $\Delta_0$-formula.

$(xxi)$: *Hint.* $\langle x, y\rangle = \{x, \{x, y\}\}$. Thus, if $\langle x, y\rangle \in A$, then $y \in \bigcup\bigcup A$.

(1): $A \times B = \{z : (\exists x \in A)(\exists y \in B) z = \langle x, y\rangle\}$. Since the defining formula is $\Delta_0$, $(A \times B)^{\mathbb{M}} = (A \times B) \cap \mathbb{M} = A \times B$, since $\mathbb{M}$ is $\{x, y\}$-closed (and hence $\langle x, y\rangle$-closed). □

**VI.8.17 Example.** Let $\mathbb{M}$ be a transitive class that is closed under pairs (hence also under *ordered* pairs), and $\mathbb{R} = \{\langle x, y\rangle : \mathscr{R}(x, y)\}$ a relation, where $\mathscr{R}$ is absolute for $\mathbb{M}$. We calculate $\mathbb{R}^{\mathbb{M}}$, noting that (cf. III.8.7)

$$\mathbb{R} = \Big\{z : (\exists x)(\exists y)\big(\langle x, y\rangle = z \wedge \mathscr{R}(x, y)\big)\Big\}$$

We have

$$\begin{aligned}
\mathbb{R}^{\mathbb{M}} &= \Big\{z \in \mathbb{M} : (\exists x \in \mathbb{M})(\exists y \in \mathbb{M})\big(\langle x, y\rangle = z \wedge \mathscr{R}(x, y)\big)\Big\}\\
&= \Big\{z : (\exists x)(\exists y)\big(\langle x, y\rangle = z \wedge z \in \mathbb{M} \wedge x \in \mathbb{M} \wedge y \in \mathbb{M} \wedge \mathscr{R}(x, y)\big)\Big\}\\
&= \Big\{z : (\exists x)(\exists y)\big(\langle x, y\rangle = z \wedge x \in \mathbb{M} \wedge y \in \mathbb{M} \wedge \mathscr{R}(x, y)\big)\Big\}\\
&= \Big\{\langle x, y\rangle : x \in \mathbb{M} \wedge y \in \mathbb{M} \wedge \mathscr{R}(x, y)\Big\}\\
&= \Big\{\langle x, y\rangle \in \mathbb{M} \times \mathbb{M} : \mathscr{R}(x, y)\Big\}\\
&= \mathbb{R} \cap (\mathbb{M} \times \mathbb{M})\\
&= \mathbb{R} \,|\, \mathbb{M}
\end{aligned}$$

The third "=" stems from the assumption that $\mathbb{M}$ is closed under pairs, which leads to the equivalence

$$\langle x, y\rangle = z \wedge z \in \mathbb{M} \wedge x \in \mathbb{M} \wedge y \in \mathbb{M} \leftrightarrow \langle x, y\rangle = z \wedge x \in \mathbb{M} \wedge y \in \mathbb{M}$$

With some practice one tends to shrug off calculations such as the above and write $\mathbb{R}^{\mathbb{M}} = \{\langle x, y\rangle \in \mathbb{M} \times \mathbb{M} : \mathscr{R}(x, y)\}$ directly. □

**VI.8.18 Example.** Continuing under the same assumptions as in VI.8.17, let moreover $\mathbb{R}$ be a function, that is, we assume (alternatively, have a proof) that

$$\mathscr{R}(x, y) \wedge \mathscr{R}(x, z) \to y = z \tag{1}$$

Tautological implication yields

$$x \in \mathbb{M} \to y \in \mathbb{M} \to z \in \mathbb{M} \to \mathscr{R}(x, y) \wedge \mathscr{R}(x, z) \to y = z$$

Hence, using assumption of absoluteness and the Leibniz rule,

$$x \in \mathbb{M} \to y \in \mathbb{M} \to z \in \mathbb{M} \to \mathscr{R}^{\mathbb{M}}(x, y) \wedge \mathscr{R}^{\mathbb{M}}(x, z) \to y = z \tag{2}$$

or (by VI.8.1)

$$x \in \mathbb{M} \to y \in \mathbb{M} \to z \in \mathbb{M} \to \big(\mathscr{R}(x, y) \wedge \mathscr{R}(x, z) \to y = z\big)^{\mathbb{M}} \tag{2$'$}$$

That is, in our jargon, "(1) is true in $\mathbb{M}$".

Let us calculate $\mathbb{R}^{\mathbb{M}}\langle a\rangle$ for $a \in \mathbb{M}$:

$$\begin{aligned}\mathbb{R}^{\mathbb{M}}\langle a\rangle &= \{x \in \mathbb{M} : \mathscr{R}^{\mathbb{M}}(a, x)\}\\ &= \{x \in \mathbb{M} : \mathscr{R}(a, x)\}\\ &= \mathbb{M} \cap \{x : \mathscr{R}(a, x)\}\\ &= \mathbb{M} \cap \mathbb{R}\langle a\rangle\end{aligned}$$

Thus, using the standard function notation "$\mathbb{R}(a)$" ($\{\mathbb{R}(a)\} = \mathbb{R}\langle a\rangle$),

$$\mathbb{R}^{\mathbb{M}}(a) \simeq \begin{cases}\uparrow & \text{if } \mathbb{R}(a) \notin \mathbb{M}\\ \mathbb{R}(a) & \text{otherwise}\end{cases} \tag{3}$$

It follows from (3) that to obtain $\mathbb{R}(a) \simeq \mathbb{R}^{\mathbb{M}}(a)$, for all $a \in \mathbb{M}$ – the absoluteness condition – we equivalently need the provability of

$$a \in \mathbb{M} \to \mathbb{R}(a) \downarrow \to \mathbb{R}(a) \in \mathbb{M}$$

that is, that $\mathbb{M}$ is $\mathbb{R}$-closed in a sense weaker than that in VI.8.1: $\mathbb{R}[\mathbb{M}] \subseteq \mathbb{M}$. In terms of $\mathscr{R}$ we need the provability of

$$x \in \mathbb{M} \to \mathscr{R}(x, y) \to y \in \mathbb{M} \tag{4}$$

An alternative notation for (4) is obtained if we set $\mathbb{D} = \mathrm{dom}(\mathbb{R})$:

$$(\forall x \in \mathbb{M} \cap \mathbb{D})\mathbb{R}(a) \in \mathbb{M} \tag{4$'$}$$

In summary, we *define* that a function $\mathbb{R} = \{\langle x, y\rangle : \mathscr{R}(x, y)\}$ is absolute for $\mathbb{M}$ (a transitive class that is closed under pairs) iff the following three conditions hold:

(i) $\mathscr{R}$ is absolute.
(ii) (1) (hence, trivially by (i), (2)) is provable.
(iii) (4) is provable.

A special case occurs if instead of the informal $\mathbb{R}$ we have introduced a formal function symbol, $\boldsymbol{R}$, by

$$y = \boldsymbol{R}(x) \leftrightarrow \mathscr{R}(x, y) \tag{5}$$

because we have a proof of

$$(\forall x)(\exists! y)\mathscr{R}(x, y) \tag{6}$$

Note that (6) combines (1) with $(\forall x)(\exists y)\mathscr{R}(x, y)$ (no "!"). Thus, our conditions for absoluteness of $\boldsymbol{R}$ – that is, (i)–(iii) – simplify to just (i) along with requiring the provability of[†]

$$\Big((\forall x)(\exists! y)\mathscr{R}(x, y)\Big)^{\mathbb{M}} \tag{7}$$

Of course, one can go back and forth between a *total* informal $\mathbb{R}$ and a formal $\boldsymbol{R}$ (cf. III.11.20); hence the two conditions (i) and (7) constitute all we need for absoluteness of a total function $\mathbb{R}$.

Finally, an interesting subcase of the formal $\boldsymbol{R}$ is that of a constant $\boldsymbol{c}$ – "0-ary function symbol" – defined by an *absolute* for $\mathbb{M}$ formula, $\mathscr{C}(y)$, as

$$\boldsymbol{c} = y \leftrightarrow \mathscr{C}(y) \tag{8}$$

after securing a proof of

$$(\exists! y)\mathscr{C}(y) \tag{9}$$

In this case the conditions of absoluteness for $\boldsymbol{c}$ are that of $\mathscr{C}$, *and* the requirement that the $\mathbb{M}$-relativization of (9) be provable. For example, if $\omega \in \mathbb{M}$, then $\omega^{\mathbb{M}} = \omega$ by VI.8.16($xv$). □

Not all absoluteness results follow from ascertaining that our formulas are $\Delta_0$. The following is an important example that does not so follow, which uses some terminology (finiteness) from the sequel, whence the ☡☡.

☡☡ **VI.8.19 Example.** A set $A$ is *finite*, formally, iff there is an onto $f : n \to A$ for some $n \in \omega$. That is,

$$\begin{aligned}\neg U(A) \wedge (\exists f)(f \text{ is a function} \wedge \operatorname{dom}(f) \text{ is a natural number}\\ \wedge(\forall y \in A)(\exists x \in \operatorname{dom}(f))\langle x, y\rangle \in f)\end{aligned} \tag{1}$$

Now, (1) is not $\Delta_0$ (and it is known that it is not equivalent to a $\Delta_0$-formula). Nevertheless, we can show that

$$\text{“}A \text{ is a finite set”} \tag{2}$$

is absolute for any transitive class $\mathbb{M}$ that satisfies a bit of ZFC. Namely, we want $\mathbb{M}$ to be closed under pairs and to contain $\omega$ ($\omega \in \mathbb{M}$). We start by observing that the formula to the right of $(\exists f)$ is $\Delta_0$. Indeed, in view of VI.8.16 one need only verify that

$$\text{“}\operatorname{dom}(f) \text{ is a natural number” is } \Delta_0 \tag{3}$$

[†] Thus, one may introduce the function symbol $\boldsymbol{R}^{\mathbb{M}}$ so that $x \in \mathbb{M} \to (y = \boldsymbol{R}^{\mathbb{M}}(x) \leftrightarrow \mathscr{R}^{\mathbb{M}}(x, y))$ and $x \notin \mathbb{M} \to \boldsymbol{R}^{\mathbb{M}}(x) = \emptyset$ are provable.

The quoted statement in (3) is *argot* for

$$\mathrm{dom}(f) = \emptyset \vee (\exists x \in \mathrm{dom}(f))\Big(\mathrm{dom}(f) = x \cup \{x\} \\ \wedge (\forall y \in \mathrm{dom}(f))(y \text{ is a natural number})\Big)$$

In view of the existential quantifier preceding it, $\mathrm{dom}(f) = x \cup \{x\}$ translates to

$$(\forall y \in x) y \in \mathrm{dom}(f) \wedge (\forall y \in \mathrm{dom}(f))(y = x \vee y \in x)$$

and we are done with claim (3). Now, by the absoluteness of the component of (1) to the right of $(\exists f)$, the relativization of the entire formula is provably equivalent to

$$\neg U(A) \wedge (\exists f \in \mathbb{M})(f \text{ is a function} \wedge \mathrm{dom}(f) \text{ is a natural number} \\ \wedge (\forall y \in A)(\exists x \in \mathrm{dom}(f))\langle x, y\rangle \in f) \tag{4}$$

To prove the absoluteness of (2), we let $A \in \mathbb{M}$ and prove the equivalence of (1) and (4). As (4) $\rightarrow$ (1) is trivial, we need worry only about (1) $\rightarrow$ (4). The whole story is to show that a “witness” $f$ for (1) (auxiliary constant) will work for (3). For the latter we only need prove $f \in \mathbb{M}$. So let $f$ be a new constant, and add the assumption

$$\neg U(A) \wedge f \text{ is a function} \wedge \mathrm{dom}(f) \text{ is a natural number} \\ \wedge (\forall y \in A)(\exists x \in \mathrm{dom}(f))\langle x, y\rangle \in f \tag{5}$$

We set $n = \mathrm{dom}(f)$ for convenience. Now transitivity of $\mathbb{M}$ and $\omega \in \mathbb{M}$ imply $n \in \mathbb{M}$ (and also $n \subseteq \mathbb{M}$). By induction on $m \le n$ we now prove $f \restriction m \in \mathbb{M}$. For $m = 0$ we are done by $0 \in \omega \in \mathbb{M}$. Taking an I.H. for $m < n$, consider $f \restriction (m \cup \{m\})$. Now,

$$f \restriction (m \cup \{m\}) = (f \restriction m) \cup \{\langle m, f(m)\rangle\}$$

and thus it is in $\mathbb{M}$ by closure under pair and absoluteness of union (VI.8.16). Thus, $f = (f \restriction n) \in \mathbb{M}$.

**Pause.** How much ZFC did we employ in the above proof? Was the assumption $\omega \in \mathbb{M}$ an overkill? If so, what would be a weaker assumption that still works? □

**VI.8.20 Example.** In our last example we consider a transitive class $\mathbb{M}$ that is a formal model of ZF, that is, we can prove, say, in ZF,

$$a_1 \in \mathbb{M} \rightarrow \cdots \rightarrow a_n \in \mathbb{M} \rightarrow \mathscr{A}^{\mathbb{M}}$$

for every ZF axiom $\mathscr{A}$ of free variables $\vec{a}_n$.[†]

[†] Therefore, $\mathfrak{J} = (L_{\mathrm{Set}}, \mathrm{ZF}, \mathbb{M})$ is the model, but it is a common abuse of terminology to say that $\mathbb{M}$ is.

If it helps the intuition, Platonistically, we may think of $\mathbb{M}$ as a (real, i.e., semantic) model of ZF, i.e., a set (or proper class) where we have interpreted $\in$ as $\in$ and $U$ as $U$, and all the ZF axioms turned out to be true.

Consider the recursive definition

$$(\forall\alpha)\mathbb{F}(\alpha) = \mathbb{G}(\mathbb{F} \restriction \alpha) \tag{1}$$

where $\mathbb{G}$ is total on $\mathbb{U}_N$, and moreover is absolute for $\mathbb{M}$. We will show that $\mathbb{F}$ is also absolute for $\mathbb{M}$ and that $\operatorname{dom}(\mathbb{F}^{\mathbb{M}}) = \mathrm{On}^{\mathbb{M}}$.

By the way,

$$\mathrm{On}^{\mathbb{M}} = \{x \in \mathbb{M} : x \text{ is an ordinal}\} = \mathbb{M} \cap \mathrm{On}, \qquad \text{by VI.8.16.} \tag{2}$$

By VI.8.18 we need to prove (in ZF), on the assumptions $x \in \mathbb{M}$, $x$ is an ordinal, and $y \in \mathbb{M}$, that

$$(y = \mathbb{F}(x))^{\mathbb{M}} \leftrightarrow y = \mathbb{F}(x) \tag{3}$$

and also (cf. (4) in VI.8.18)

$$x \in \mathbb{M} \wedge (x \text{ is an ordinal}) \rightarrow \mathbb{F}(x) \in \mathbb{M} \tag{4}$$

Note that the first two assumptions, in view of (2), are jointly equivalent to $x \in \mathrm{On}^{\mathbb{M}}$. We can then use, as usual, $\alpha$ to mean "$x \in \mathrm{On}$ and $x = \alpha$".

By the proof of VI.5.16,[†] $y = \mathbb{F}(\alpha)$ stands for

$$\begin{aligned}(\exists! f)\Big(& f \text{ is a function} \wedge \operatorname{dom}(f) = \alpha \cup \{\alpha\} \\ & \wedge \big(\forall\beta \in \alpha \cup \{\alpha\}\big)\mathscr{G}(f \restriction \beta, f(\beta)) \wedge \langle\alpha, y\rangle \in f\Big)\end{aligned} \tag{5}$$

Consulting the list VI.8.16 and also invoking VI.8.14, we observe that, for $\alpha$ and $y$ in $\mathbb{M}$, the relativization of (5) – *within provable equivalence* – introduces only one annoying part, namely, $(\exists! f \in \mathbb{M})$.[‡]

Let then $\underline{\alpha \in \mathbb{M} \text{ and } y \in \mathbb{M}.}$ The relativization of (5) is (provably equivalent to)

$$\begin{aligned}(\exists! f \in \mathbb{M})\Big(& f \text{ is a function} \wedge \operatorname{dom}(f) = \alpha \cup \{\alpha\} \\ & \wedge \big(\forall\beta \in \alpha \cup \{\alpha\}\big)\mathscr{G}(f \restriction \beta, f(\beta)) \wedge \langle\alpha, y\rangle \in f\Big)\end{aligned} \tag{6}$$

[†] Actually, no detailed proof was given for this particular statement. The detailed proof that applies here as well, with only notational modifications, was given in VI.2.25 for a more general case of recursion, not just for recursion over On.

[‡] Note that the term $f \restriction x$ is short for $\{z : \pi(z) \in x \wedge z \in f\}$, that is, $\{z : ((\exists y \in x) y = \pi(z)) \wedge z \in f\}$, and is thus absolute, and defined in $\mathbb{M}$ on the assumptions $x \in \mathbb{M}$ and $f \in \mathbb{M}$. Thus VI.8.14 applies.

which we abbreviate as

$$(\exists! f \in \mathbb{M})\mathscr{C}(f, \alpha, y) \tag{6$'$}$$

in what follows. We will have shown (3) if we prove, under our underlined assumptions, that (5) → (6′), the other direction being trivial.

Add then (5) as an assumption, as well as a new constant $g$ and the assumption

$$\mathscr{C}(g, \alpha, y) \tag{5$'$}$$

In VI.5.16 we gave a proof in ZF

**Pause.** In ZF? Is this true?

that

$$(\forall\alpha)(\exists! y)(\exists! f)\mathscr{C}(f, \alpha, y) \tag{7}$$

Since $\mathbb{M}$ is a formal model of ZF, and being mindful of the relativization claims we made a few steps back, we have (by I.7.9) a ZF-proof of

$$(\forall\alpha \in \mathbb{M})(\exists! y \in \mathbb{M})(\exists! f \in \mathbb{M})\mathscr{C}(f, \alpha, y) \tag{8}$$

Specializing (8), we derive $(\exists y \in \mathbb{M})(\exists f \in \mathbb{M})\mathscr{C}(f, \alpha, y)$.

Thus, adding two new constants $c$ and $h$, we may add also

$$\mathscr{C}(h, \alpha, c) \tag{9}$$

and

$$h \in \mathbb{M} \tag{10}$$

Now, the "!"-notation in (7) is short for $(\forall\alpha)(\exists y)(\exists f)\mathscr{C}(f, \alpha, y)$ *and*

$$\mathscr{C}(f, \alpha, y) \rightarrow \mathscr{C}(f', \alpha, y') \rightarrow f = f' \wedge y = y' \tag{11}$$

Thus, since we have (7), the above and (5′) yield $y = c$ and $h = g$; hence, from (10), $g \in \mathbb{M}$. We have derived (cf. (5′))

$$g \in \mathbb{M} \wedge \mathscr{C}(g, \alpha, y)$$

and hence (6′) by the substitution axiom (the "!" is inserted by (11)).

So $y = \mathbb{F}(\alpha)$ is absolute. We need to establish (4) to show that $\mathbb{F}$ is. In fact, (4) is a direct result of (8), which also yields $\mathrm{dom}(\mathbb{F}^{\mathbb{M}}) = \mathbb{M} \cap \mathrm{On} = \mathrm{On}^{\mathbb{M}}$. □ ☡☡

☡☡ **VI.8.21 Exercise.** As an important application of the above, prove that $TC(x)$ is absolute for any transitive formal model of ZF, $\mathbb{M}$.

*Hint.* Recall that

$$TC(x) = x \cup \bigcup x \cup \bigcup\bigcup x \cup \bigcup\bigcup\bigcup \cup \cdots$$

Express the above as a recursive definition (you only need recursion in $\omega$, but to fit the result in the style of the previous example, define your function in a trivial way for arguments $\geq \omega$). □

**VI.8.22 Exercise.** Prove (in ZF) that $TC$ satisfies

$$U(x) \to TC(x) = \emptyset$$

and

$$\neg U(x) \to TC(x) = x \cup \bigcup \{TC(y) : y \in x\}$$ □

**VI.8.23 Exercise (Induction on $TC(x)$).** Prove that for any formula $\mathscr{F}(x)$,[†]

$$\vdash_{ZF} (\forall x)\Big((\forall y \in TC(x))\mathscr{F}(y) \to \mathscr{F}(x)\Big) \to (\forall x)\mathscr{F}(x)$$

That is, to prove $\mathscr{F}(x)$ we are helped by the assumption $(\forall y \in TC(x))\mathscr{F}(y)$ that we can add for free.

*Hint.* Start by assuming the hypothesis and proving using foundation (equivalently, $\in$-induction) that $\vdash_{ZF} (\forall x)(\forall y \in TC(x))\mathscr{F}(y)$. □

**VI.8.24 Exercise.** Another important application of the technique in VI.8.20 is the following: First, *working in ZF*, assume that $(\forall x)(\exists! y)\mathscr{G}(x, y)$, and prove that a unique informal *total* function $\mathbb{F}$ exists (equivalently, you may introduce a (formal) unary function symbol, $\boldsymbol{F}$, for $\mathbb{F}$) such that

$$(\forall x)\mathbb{F}(x) = \mathbb{G}\big(\mathbb{F} \restriction TC(x)\big) \tag{1}$$

where we have written $\mathbb{G}$ for the function given by $y = \mathbb{G}(x) \leftrightarrow \mathscr{G}(x, y)$ (we could also have introduced a formal $\boldsymbol{G}$).

*Hint.* Imitate the proof of VI.2.25. Start by showing that $y = \mathbb{F}(x)$ (or $y = \boldsymbol{F}(x)$) must stand for

$$(\exists! f)\mathscr{C}(f, x, y)$$

where $\mathscr{C}(f, x, y)$ abbreviates

$$\begin{aligned}
&f \text{ is a function} \wedge \mathrm{dom}(f) = TC(x) \wedge \\
&(\forall z \in TC(x))\mathscr{G}(f \restriction TC(z), f(z)) \wedge \\
&f(x) = y
\end{aligned}$$

[†] This works in weaker set theories. For example, neither infinity nor power set axioms are required.

You will need to show that

$$\vdash_{\mathrm{ZF}} (\forall x)(\exists! y)(\exists! f)\mathscr{C}(f, x, y)$$

Once the fact that $\mathbb{F}$ (or $\boldsymbol{F}$) can be introduced has been established, show that $\mathbb{F}$ is absolute for any transitive formal model of ZF for which $\mathbb{G}$ is absolute. This will imitate the work in VI.8.20. We know that $TC(x)$ is absolute by VI.8.21. We need to worry about things such as $(\exists y \in TC(x))$, $y \in TC(x)$, and $\mathrm{dom}(f) = TC(x)$. □

**VI.8.25 Exercise (Absoluteness of Rank).** Prove in ZF that the rank $\rho$ is absolute for transitive formal models of ZF. Do so by bringing the recursive definition of rank (cf. VI.6.24) into the form (1) in VI.8.24. Treat $N$ as a parameter. □

**VI.8.26 Exercise.** Prove in ZF that the function $J$ as well as the various $\pi_i^n$ of Section VI.7 are absolute for transitive formal models of ZF.

*Hint.* $J$ satisfies the recurrence

$$(\forall x \in \mathrm{On})(\forall y \in \mathrm{On})J(x, y) = \{J(x', y') : \langle x', y'\rangle \in \mathrm{On}^2 \wedge \langle x', y'\rangle \lhd \langle x, y\rangle\}$$

or

$$(\forall x \in \mathrm{On})(\forall y \in \mathrm{On})J(x, y) = \mathrm{ran}\left(J \restriction \lhd\big\langle\langle x, y\rangle\big\rangle\right)$$

Absoluteness follows (after some work) from our standard technique that proves the existence of recursively defined functions: Start by proving in ZF that $J(\alpha, \beta) = \gamma$ must be given by

$$(\exists! f)\mathscr{C}(f, \alpha, \beta, \gamma)$$

where

$$\begin{aligned}\mathscr{C}(f, \alpha, \beta, \gamma) \leftrightarrow\ & f \text{ is a function} \wedge \mathrm{dom}(f) = \lhd\big\langle\langle \alpha, \beta\rangle\big\rangle \cup \{\langle \alpha, \beta\rangle\} \wedge \\ & (\forall w \in \mathrm{dom}(f)) f(w) = \mathrm{ran}\left(f \restriction \lhd\big\langle w\big\rangle\right) \wedge \\ & f(\langle \alpha, \beta\rangle) = \gamma\end{aligned}$$

As in all previous cases where this technique was employed, $f$ simply "codes" the computation that verifies $J(\alpha, \beta) = \gamma$. Now you will need a few absoluteness lemmata to conclude your case. For example, you will need the absoluteness of $x \in \lhd\big\langle\langle\alpha, \beta\rangle\big\rangle$. This is equivalent to

$$\begin{aligned}
&OP(x) \wedge \pi(x) \in \mathrm{On} \wedge \delta(x) \in \mathrm{On} \wedge \\
&\quad \big[\big((\pi(x) \in \alpha \vee \pi(x) \in \beta) \wedge (\delta(x) \in \alpha \vee \delta(x) \in \beta)\big) \vee \\
&\quad \big(\pi(x) \cup \delta(x) = \alpha \cup \beta \wedge (\pi(x) < \alpha \vee \pi(x) = \alpha \wedge \delta(x) < \beta)\big)\big]
\end{aligned}$$

etc. □

## VI.9. The Constructible Universe

We now revisit Section IV.2 from a formal point of view. The quest there was simply to show that AC is plausible, but here we will do more.

We will define a cumulative hierarchy of sets, similar to the von Neumann hierarchy, but as in Section IV.2 – and unlike what we did in Section VI.6 – we will be careful not to admit *all* the sets that a "powering stage" yields.[†] We will accept instead only those sets that can be defined by *explicit* and "simple" operations based on what is available "so far". This is one of the differences. The other essential difference is that *no two sets are constructed at the same stage* (even the urelements will be given at distinct stages).

The construction will build a formal model, $\mathfrak{J} = (L_{\mathrm{Set}}, \mathrm{ZF}, \mathbb{L}_N)$ of ZFC, where, as in Section VI.6, $\in$ will be interpreted as $\in$ and $U$ as $U$.[‡] The proof of AC in the model will be, unlike the informal argument of Section IV.2, a consequence of the fact that a construction stage produces a unique constructible object. In particular, all this work will establish that if ZF is consistent, then so is ZFC (cf. Section I.7), i.e., adding AC doesn't hurt a theory that is not already broken.

The whole idea of the construction of $\mathfrak{J}$ is due to Gödel (1938, 1939, 1940), who gave two different constructions, one outlined in Section IV.2, the other to be followed here. The story has been retold by many, in many slightly different ways. Our version is influenced by the accounts given by Shoenfield (1967), Barwise (1975), and Jech (1978b).

After these preliminaries, we embark now upon the construction of Gödel's constructible universe $\mathbb{L}_N$ over any *appropriately chosen* set of urelements $N$. Sets will be built by iterating some simple "explicit" operations (Gödel operations). There have being many variations in the choice of these operations. The following definition is one of these variations (close to the version

[†] These are in $V_N(\alpha + 1) = \mathbf{P}(N \cup V_N(\alpha))$ when we start with the set of urelements $N$.

[‡] Thus, $\mathfrak{J}$ will be a so-called $\in$-model, or more accurately, $(U, \in)$-model.

in Shoenfield (1967), but with some departures for convenience and user-friendliness).

**VI.9.1 Definition (The Gödel Operations).** We call the terms $\mathfrak{F}_i$ below the *Gödel operations*:

$$\begin{aligned}
\mathfrak{F}_0(x, y) &= x - y \\
\mathfrak{F}_1(x, y) &= x \cap \mathrm{dom}(y) \\
\mathfrak{F}_2(x, y) &= \{z \in x : U(z)\} \\
\mathfrak{F}_3(x, y) &= \{\langle u, v\rangle \in x : u = v\} \\
\mathfrak{F}_4(x, y) &= \{\langle u, v\rangle \in x : u \in v\} \\
\mathfrak{F}_5(x, y) &= \{\langle u, v\rangle \in x : \langle v, u\rangle \in y\} \\
\mathfrak{F}_6(x, y) &= \{\langle u, v, w\rangle \in x : \langle v, w, u\rangle \in y\} \\
\mathfrak{F}_7(x, y) &= \{\langle u, v, w\rangle \in x : \langle u, w, v\rangle \in y\} \\
\mathfrak{F}_8(x, y, z) &= x \cap (y \times z) \\
\mathfrak{F}_9(x, y) &= \{x, y\}
\end{aligned}$$

□

The purpose of the Gödel operations is to provide "normalized" terms which by repeated composition (substitution of one into the other) will form all the "constructible" sets.

Indices 2–4 take care of the atomic formulas of set theory. Indices 5–7 ensure that we can manipulate "vectors", and, in particular, provide tools to address the fact that $\langle u, v, w\rangle \neq \langle u, \langle v, w\rangle\rangle$. Note the absence of power set operations (we want to provide subsets in a "controlled" manner). Note also that for each $i = 0, \ldots, 7$, $\mathfrak{F}_i(x, y) \subseteq x$, and $\mathfrak{F}_8(x, y, z) \subseteq x$, a "technical" fact from which we will benefit (cf. VI.9.3 below). This technicality compelled the choice of the rather awkward $x \cap \mathrm{dom}(y)$ and $x \cap (y \times z)$ instead of just $\mathrm{dom}(y)$ and $y \times z$ at indices 1 and 8.

**VI.9.2 Definition (The Sets Constructible from $N$).** Fix a set $N$ of urelements and a function $f$ such that $N \overset{f}{\simeq} \|N\|$, where we have written $\|N\|$ for $\mathrm{dom}(f)$, an ordinal.[†]

[†] This means the following: On one hand, trivially, $\vdash_{ZF} (\exists x)(\exists y)(\neg U(x) \wedge (\forall z \in x)U(z) \wedge y$ is a 1-1 function $\wedge\ \mathrm{dom}(y) \in \mathrm{On} \wedge \mathrm{ran}(y) = x)$. For example, $x = y = \emptyset$ work, and then we can invoke the substitution axiom. Now one can introduce new constants $N$ and $f$ along with assumption (cf. p. 75),

$$\neg U(N) \wedge (\forall z \in N)U(z) \wedge f \text{ is a 1-1 function} \wedge \mathrm{dom}(f) \in \mathrm{On} \wedge \mathrm{ran}(f) = N$$

Define by recursion over On the function $\alpha \mapsto F_\alpha$:

$$\begin{array}{lrll}
\text{for } \alpha < \|N\| : & F_\alpha & = f(\alpha), & \\
\text{for } \alpha \geq \|N\| : & F_\alpha & = \bigcup_{\|N\| \leq \beta < \alpha} F_\beta & \text{if } \mathrm{Lim}(\alpha) \vee \alpha = 0 \\
\text{for } \alpha + 1 \geq \|N\| : & F_{\alpha+1} & = \mathfrak{F}_i(F_{\pi_1^4(\alpha)}, F_{\pi_2^4(\alpha)}) & \text{if } \pi_4^4(\alpha) = i < 8 \\
 & F_{\alpha+1} & = \mathfrak{F}_8(F_{\pi_1^4(\alpha)}, F_{\pi_2^4(\alpha)}, F_{\pi_3^4(\alpha)}) & \text{if } \pi_4^4(\alpha) = 8 \\
 & F_{\alpha+1} & = \mathfrak{F}_9(F_{\pi_1^4(\alpha)}, F_{\pi_2^4(\alpha)}) & \text{if } \pi_4^4(\alpha) \geq 9
\end{array}$$

where the $\pi_i^n$ are those of VI.7.5.

An *object* $x$ (i.e., set or urelement) is *constructible* (*from* $N$ – a qualification that is omitted if it is clear from the context) just in case $x = F_\alpha$ for some $\alpha$. We will also say that $x$ is $N$-constructible.

$\mathbb{L}_N$ is the class of *all objects* constructible from $N$ (if $N = \emptyset$, then we write $\mathbb{L}$ rather than $\mathbb{L}_\emptyset$).

We will use the notation $\mathrm{ord}(x)$ to indicate $\min\{\alpha : F_\alpha = x\}$. We will pronounce $\mathrm{ord}(x)$ "order of $x$". □

The previous recursive definition is appropriate, since $\pi_i^4(\alpha) \leq \alpha < \alpha + 1$ for $i = 1, 2, 3, 4$ (see VI.7.7). It uses ordinals to systematically iterate the Gödel operations "as long as possible". In this section we work in ZF; thus we had to *ask* that $N$ be well-ordered (in ZFC, of course, every set is well-orderable by Zermelo's theorem). The subcase "$\vee\, \alpha = 0$" (part of the case "for $\alpha \geq \|N\|$") takes care of the situation where $N = \emptyset$. Then $F_0 = \emptyset$.

The reader will want to compare the above definition with Definition VI.6.1. $\mathbb{L}_N$ parallels $\mathbb{U}_N$ (rather than $\mathbb{V}_N$). The major differences between the two definitions are:

(1) Instead of using the power set operation at successor ordinal stages, we are using explicit (Gödel) operations that are much "weaker" than forming power sets, to construct *one* member of the hierarchy at a time.
(2) The urelements are not given at once (stage 0), but are "built" one at a time; it takes $\|N\|$ steps to have them all.

Between successive limit ordinals we ensure that each case (among the ten Gödel operations) gets "equal opportunity" to apply (at successor ordinal stages), by using a technique recursion theorists call "dovetailing".[†]

[†] For each case, according as $\pi_4^4(\alpha) = 0, 1, \ldots, 8$, or $> 8$, *all* pairs $\langle \pi_1^4(\alpha), \pi_2^4(\alpha) \rangle$ and all triples $\langle \pi_1^4(\alpha), \pi_2^4(\alpha), \pi_3^4(\alpha) \rangle$ will be considered, since $\alpha \mapsto \langle \pi_1^4(\alpha), \pi_2^4(\alpha), \pi_3^4(\alpha), \pi_4^4(\alpha) \rangle$ is onto – as follows from VI.7.5 by the observation that $\langle K, L \rangle$ is onto.

Note that $\operatorname{ord}(x)$ is similar to $\rho(x)$ of VI.6.19, but it is a different function here, whence the different symbol.

We easily see by induction on $\alpha$ that $\vdash_{\mathrm{ZF}} sp(F_\alpha) \subseteq N$.

The following few lemmata are central:

**VI.9.3 Lemma.** *Let $x \in \mathbb{L}_N$. Then $y \in x$ implies $y \in \mathbb{L}_N$ and* $\operatorname{ord}(y) < \operatorname{ord}(x)$.

*Proof.* We do induction on $\operatorname{ord}(x)$, setting $\gamma = \operatorname{ord}(x)$ for convenience.

If $\gamma < \|N\|$ or $\|N\| \le \gamma = 0$, then the claim is vacuously satisfied.

Let then $\gamma \ge \|N\|$ and $\operatorname{Lim}(\gamma)$. By VI.9.2, $x = \bigcup_{\|N\| \le \beta < \gamma} F_\beta$. Then $y \in x$ implies $y \in F_\beta$ for some $\|N\| \le \beta < \gamma$. By the obvious I.H. (since $\operatorname{ord}(F_\beta) \le \beta < \gamma$), we have $y \in \mathbb{L}_N$ and $\operatorname{ord}(y) < \operatorname{ord}(F_\beta) < \gamma = \operatorname{ord}(x)$.

Let $\gamma = \alpha + 1 \ge \|N\|$. We have cases according to $i = \pi_4^4(\alpha)$:

$$y \in x = F_{\alpha+1} = \begin{cases} \mathfrak{F}_i(F_{\pi_1^4(\alpha)}, F_{\pi_2^4(\alpha)}) & \text{if } i = 0, \ldots, 7 \\ \mathfrak{F}_i(F_{\pi_1^4(\alpha)}, F_{\pi_2^4(\alpha)}, F_{\pi_3^4(\alpha)}) & \text{if } i = 8 \end{cases}$$

Then

$$y \in x \subseteq F_{\pi_1^4(\alpha)}$$

by VI.9.1. By the obvious I.H. (note that $\operatorname{ord}(F_{\pi_1^4(\alpha)}) \le \pi_1^4(\alpha) \le \alpha < \alpha + 1$), we have $y \in \mathbb{L}_N$ and $\operatorname{ord}(y) < \operatorname{ord}(F_{\pi_1^4(\alpha)}) < \alpha + 1 = \operatorname{ord}(x)$.

Finally, let $y \in x = F_{\alpha+1} = \mathfrak{F}_9(F_{\pi_1^4(\alpha)}, F_{\pi_2^4(\alpha)})$. Then $y = F_{\pi_j^4(\alpha)}$ for $j = 1$ or $j = 2$; hence $\operatorname{ord}(y) = \operatorname{ord}(F_{\pi_j^4(\alpha)}) \le \pi_j^4(\alpha) \le \alpha < \alpha + 1$. Moreover, $y \in \mathbb{L}_N$, since it is an "$F_\beta$". □

**VI.9.4 Corollary.** *$\mathbb{L}_N$ is a transitive class.*

**VI.9.5 Lemma.** *$\mathbb{L}_N$ is closed under $\mathfrak{F}_i$ for $i = 0, \ldots, 9$.*

*Proof.* Straightforward index computations, and VI.9.2, yield this claim. For example, say that $x, y$ (sets or atoms) are in $\mathbb{L}_N$, so that $x = F_\alpha$ and $y = F_\beta$. Then $J_4(\alpha, \beta, \|N\|, 9) \ge \|N\|$ (by VI.7.7) and

$$\mathbb{L}_N \ni F_{J_4(\alpha,\beta,\|N\|,9)+1} = \mathfrak{F}_9(x, y) = \{x, y\}$$

Note, in particular, that

$$\mathbb{L}_N \ni F_{J_4(\alpha,\alpha,\|N\|,9)+1} = \mathfrak{F}_9(x, x) = \{x\}$$

Similarly, if $x$, $y$ are sets with orders as above, $x \cap \operatorname{dom}(y) = F_{J_4(\alpha,\beta,1,1)+1}$ (why is $J_4(\alpha, \beta, 1, 1) + 1 \geq \|N\|$?) The remaining cases are left to the reader. □

**VI.9.6 Corollary.** *If each $x_i$ $(i = 1, \ldots, n)$ is in $\mathbb{L}_N$, so is $\langle x_1, x_2, \ldots, x_n\rangle$.*

This is a theorem schema: one theorem for each $n \in \mathbb{N}$. The proof is by informal induction on $n$.

*Proof.* Induction on $n$. For $n = 1$, $\langle x_1\rangle = x_1$ and there is nothing to prove. We proceed to $n + 1$ via (I.H.) $n$: Now $\langle u, v\rangle = \{u, \{u, v\}\}$; hence it is in $\mathbb{L}_N$ whenever $u$, $v$ are. Thus, $\langle x_1, \ldots, x_{n+1}\rangle = \langle\langle x_1, \ldots, x_n\rangle, x_{n+1}\rangle \in \mathbb{L}_N$ by I.H. □

**VI.9.7 Lemma.** *If $x$ is a* set *and $x \subseteq \mathbb{L}_N$, then there is a set $y \in \mathbb{L}_N$ such that $x \subseteq y$.*

*Proof.* The hypothesis yields, via Lemma VI.9.5,

$$(\forall z \in x)(\exists\alpha)\{z\} = F_\alpha$$

By collection, there is a set $A$ such that

$$(\forall z \in x)(\exists\alpha \in A)\{z\} = F_\alpha$$

Let $\gamma = \bigcup_{\alpha\in A} \alpha$ (VI.5.22). Borrowing two results from the next section (VI.10.3 and VI.10.11), we note that $\operatorname{Lim}(\gamma + \omega)$ and $\gamma < \gamma + \omega$. Thus

$$y = F_{\gamma+\omega} = \bigcup_{\|N\|\leq\alpha<\gamma+\omega} F_\alpha$$

will do. □

**VI.9.8 Lemma.** *$\mathbb{L}_N$ is closed under $\cap$, $\cup$, and $\times$.*

*Proof.* Let the sets $x$, $y$ be in $\mathbb{L}_N$. Then $x \cap y = x - (x - y) = \mathfrak{F}_0(x, \mathfrak{F}_0(x, y))$; thus it is in $\mathbb{L}_N$ by VI.9.5.

Closure under $\cup$ follows by this argument: $x \cup y \subseteq \mathbb{L}_N$ (by transitivity of $\mathbb{L}_N$); hence (VI.9.7), for some $z \in \mathbb{L}_N$, $x \cup y \subseteq z$. But then, $x \cup y = (z - x) \cap (z - y)$.

Finally, $x \times y \subseteq \mathbb{L}_N$, by VI.9.3 and VI.9.6. Thus, for some $z \in \mathbb{L}_N$, $x \times y \subseteq z$. Hence $x \times y = (x \times y) \cap z = \mathfrak{F}_8(z, x, y)$. □

**Pause.** But what about $x \cap y$ when, say, $U(x)$? We have said in Chapter III that the formal operations ($\cap$, $\cup$, $-$) are total, so they make sense on atoms (in $N$) too.

**VI.9.9 Lemma.** $\mathbb{L}_N$ *is closed under* dom.

*Proof.* Let $x \in \mathbb{L}_N$ and $z \in x$. By two applications of VI.9.3, $\pi(z)$, i.e., the $y$ which for some $w$ satisfies $z = \{y, \{y, w\}\} \in x$, is in $\mathbb{L}_N$. Thus, $\operatorname{dom}(x) \subseteq \mathbb{L}_N$ and, of course, $\operatorname{dom}(x)$ is a set by collection. Thus (VI.9.7), for some $u \in \mathbb{L}_N$, $\operatorname{dom}(x) \subseteq u$, and hence we are done by (VI.9.5), since $\operatorname{dom}(x) = \operatorname{dom}(x) \cap u = \mathfrak{F}_1(u, x)$. □

**VI.9.10 Lemma (Three "Derived" Gödel Operations).** $\mathbb{L}_N$ *is closed under*

$$\begin{aligned}
\mathfrak{F}_{10}(x) &= \{\langle u, v\rangle : \langle v, u\rangle \in x\}\\
\mathfrak{F}_{11}(x) &= \{\langle u, v, w\rangle : \langle v, w, u\rangle \in x\}\\
\mathfrak{F}_{12}(x) &= \{\langle u, v, w\rangle : \langle u, w, v\rangle \in x\}
\end{aligned}$$

*Proof.* Let $x$ be in $\mathbb{L}_N$. Using VI.9.3, collection, and VI.9.7, we have sets $y_1, y_2, y_3$ in $\mathbb{L}_N$ such that

$$\begin{aligned}
\mathfrak{F}_{10}(x) &\subseteq y_1\\
\mathfrak{F}_{11}(x) &\subseteq y_2\\
\mathfrak{F}_{12}(x) &\subseteq y_3
\end{aligned}$$

Thus, $\mathfrak{F}_{10}(x) = \mathfrak{F}_5(y_1, x)$, $\mathfrak{F}_{11}(x) = \mathfrak{F}_6(y_2, x)$, and $\mathfrak{F}_{12}(x) = \mathfrak{F}_7(y_3, x)$. We are done by VI.9.5. □

The following lemma shows that introducing dummy variables does not take us out of $\mathbb{L}_N$. It forms the fundamental step of the main result of this section, that $\mathbb{L}_N$ is a model of ZFC, in that it helps to show that $\mathbb{L}_N$ satisfies the separation axiom.

**VI.9.11 Lemma.** *For all $n \geq 1$, all $i, j$ among $1, \ldots, n$, and all $N$-constructible sets $a_1, \ldots, a_n$, $b$, the set*

$$\mathfrak{F}^{(n)}(a_1, \ldots, a_n) = \{\langle u_1, \ldots, u_n\rangle \in a_1 \times \cdots \times a_n : \langle u_i, u_j\rangle \in b\}$$

*is in* $\mathbb{L}_N$.

This too is a theorem schema.

*Proof.* Let first $i \neq j$. We do (informal) induction on the length of $\langle u_1, \ldots, u_n\rangle$.

For the basis, we have $n = 2$, and the result follows from VI.9.8 and VI.9.5 on observing that

$$\mathfrak{F}^{(2)}(a_1, a_2) = \{\langle u_1, u_2\rangle \in a_1 \times a_2 : \langle u_1, u_2\rangle \in b\} = (a_1 \times a_2) \cap b$$

if $i < j$, and

$$\begin{aligned}\mathfrak{F}^{(2)}(a_1, a_2) &= \{\langle u_1, u_2\rangle \in a_1 \times a_2 : \langle u_2, u_1\rangle \in b\}\\ &= \mathfrak{F}_5(a_1 \times a_2, b)\end{aligned}$$

otherwise.

For the induction step we consider cases.

*Case $n \notin \{i, j\}$.* By I.H.,

$$\mathfrak{F}^{(n-1)}(a_1, \ldots, a_{n-1}) = \{\langle u_1, \ldots, u_{n-1}\rangle \in a_1 \times \cdots \times a_{n-1} : \langle u_i, u_j\rangle \in b\}$$

is in $\mathbb{L}_N$. But then so is

$$\mathfrak{F}^{(n)}(a_1, \ldots, a_n) = \mathfrak{F}^{(n-1)}(a_1, \ldots, a_{n-1}) \times a_n$$

by VI.9.8.

*Case $n \in \{i, j\}$ and $i, j$ are consecutive integers.* If $n = 2$, then we are back to the basis step, so assume $n > 2$. Now, observe that $\langle u_1, \ldots, u_{n-1}, u_n\rangle = \langle\langle u_1, \ldots, u_{n-2}\rangle, u_{n-1}, u_n\rangle$, and set

$$\begin{aligned}&\mathfrak{F}^{(3)}\big(a_{n-1}, a_n, (a_1 \times \cdots \times a_{n-2})\big)\\ &\quad = \{\langle u_{n-1}, u_n, \langle u_1, \ldots, u_{n-2}\rangle\rangle \in (a_{n-1} \times a_n)\\ &\qquad \times (a_1 \times \cdots \times a_{n-2}) : \langle u_i, u_j\rangle \in b\}\end{aligned}$$

Clearly, $\mathfrak{F}^{(3)}\big(a_{n-1}, a_n, (a_1 \times \cdots \times a_{n-2})\big) \in \mathbb{L}_N$ by the previous case (and VI.9.8), and

$$\begin{aligned}\mathfrak{F}^{(n)}(a_1, \ldots, a_n) &= \{\langle u_1, \ldots, u_n\rangle \in a_1 \times \cdots \times a_n : \langle u_i, u_j\rangle \in b\}\\ &= \mathfrak{F}_{11}\Big(\mathfrak{F}^{(3)}\big(a_{n-1}, a_n, (a_1 \times \cdots \times a_{n-2})\big)\Big)\end{aligned}$$

Therefore, the latter is in $\mathbb{L}_N$ by VI.9.10.

*Case $n \in \{i, j\}$ and $i, j$ are not consecutive integers.* By the first case,

$$\begin{aligned}\widetilde{\mathfrak{F}^{(n)}}(a_1, \ldots, a_n) = \{\langle u_1, \ldots, u_n, u_{n-1}\rangle \in&\\ a_1 \times \cdots \times a_n \times a_{n-1} : \langle u_i, u_j\rangle \in b\}&\end{aligned}$$

is in $\mathbb{L}_N$. Since $\langle u_1, \ldots, u_{n-1}, u_n\rangle = \langle\langle u_1, \ldots, u_{n-2}\rangle, u_{n-1}, u_n\rangle$, we conclude that

$$\begin{aligned}\mathfrak{F}^{(n)}(a_1, \ldots, a_n) &= \{\langle u_1, \ldots, u_{n-1}, u_n\rangle \in a_1 \times \cdots \times a_n : \langle u_i, u_j\rangle \in b\}\\ &= \mathfrak{F}_{12}\big(\widetilde{\mathfrak{F}^{(n)}}(a_1, \ldots, a_n)\big)\end{aligned}$$

is in $\mathbb{L}_N$.

*Case $i = j$, finally.* By VI.9.5 and VI.9.8,

$$\begin{aligned}\mathfrak{F}^{(2)}(a_i, a_i) &= \{\langle u_i, u_i\rangle \in a_i \times a_i : \langle u_i, u_i\rangle \in b\}\\ &= \mathfrak{F}_3(c, c)\end{aligned}$$

where $c = a_i \cap b$, is in $\mathbb{L}_N$. Clearly, $\langle u_i, u_i\rangle \in \mathfrak{F}_3(c, c)$ iff $u_i \in \mathrm{dom}(\mathfrak{F}_3(c, c))$. Thus,

$$\mathfrak{F}^{(n)}(a_1, \ldots, a_n) = a_1 \times \cdots \times a_{i-1} \times \mathrm{dom}(\mathfrak{F}_3(c, c)) \times a_{i+1} \times \cdots \times a_n$$

where, without loss of generality, we have assumed that $i$ is " in general position" $(1 < i < n)$.[†] The result follows from VI.9.9. □

We need one more lemma before we can successfully tackle separation in $\mathbb{L}_N$.

**VI.9.12 Lemma.** *For each $n \geq 1$ and $N$-constructible sets $a_1, \ldots, a_n$ and for each formula $\mathscr{A}(\vec{u}_n)$ of set theory, the set*

$$\mathfrak{F}_{\mathscr{A}}(a_1, \ldots, a_n) = \{\langle u_1, \ldots, u_n\rangle \in a_1 \times \cdots \times a_n : \mathscr{A}^{\mathbb{L}_N}(\vec{u}_n)\}$$

*is in $\mathbb{L}_N$.*

Some of the arguments in $\mathscr{A}(\vec{u}_n)$ might be dummy ones, as in $\lambda u_1 u_2 u_3.u_3 \in u_1$. The round brackets, according to our earlier conventions, mean that – dummy or not – "$\vec{u}_n$" is the *entire list of variables* relevant to $\mathscr{A}$.

*Proof.* We do induction on formulas $\mathscr{A}$. The reader will want to keep in mind Definition VI.8.1.

*Case $\mathscr{A}(\vec{u}_n)$ is $\lambda\vec{u}_n.U(u_i)$.* Then, since $U^{\mathbb{L}_N}(x)$ is $U(x)$, we obtain

$$\begin{aligned}\mathfrak{F}_{\mathscr{A}}(a_1, \ldots, a_n) &= \{\langle u_1, \ldots, u_n\rangle \in a_1 \times \cdots \times a_n : U(u_i)\}\\ &= a_1 \times \cdots \times a_{i-1} \times \mathfrak{F}_2(a_i, a_i) \times a_{i+1} \times \cdots \times a_n\end{aligned}$$

in $\mathbb{L}_N$, by VI.9.5 and VI.9.8.

[†] Of course, "×" associates left to right, and we omitted brackets to avoid cluttering the notation.

*Case $\mathscr{A}(\vec{u}_n)$ is $\lambda\vec{u}_n.u_i = u_j$ (possibly $i = j$).* Then, since $(x = y)^{\mathbb{L}_N}$ is $x = y$, we obtain

$$\begin{aligned}&\mathfrak{F}_{\mathscr{A}}(a_1, \ldots, a_n)\\ &\qquad = \{\langle u_1, \ldots, u_n\rangle \in a_1 \times \cdots \times a_n : u_i = u_j\}\\ &\qquad = \{\langle u_1, \ldots, u_n\rangle \in a_1 \times \cdots \times a_n : \langle u_i, u_j\rangle \in \mathfrak{F}_3(a_i \times a_j, a_i)\}\end{aligned}$$

in $\mathbb{L}_N$, by VI.9.5, VI.9.8, and VI.9.11.

*Case $\mathscr{A}(\vec{u}_n)$ is $\lambda\vec{u}_n.u_i \in u_j$ (possibly $i = j$).* Then, since $(x \in y)^{\mathbb{L}_N}$ is $x \in y$, we obtain

$$\begin{aligned}&\mathfrak{F}_{\mathscr{A}}(a_1, \ldots, a_n)\\ &\qquad = \{\langle u_1, \ldots, u_n\rangle \in a_1 \times \cdots \times a_n : u_i \in u_j\}\\ &\qquad = \{\langle u_1, \ldots, u_n\rangle \in a_1 \times \cdots \times a_n : \langle u_i, u_j\rangle \in \mathfrak{F}_4(a_i \times a_j, a_i)\}\end{aligned}$$

in $\mathbb{L}_N$, by VI.9.5, VI.9.8, and VI.9.11.

*Case $\mathscr{A}(\vec{u}_n)$ is $\neg\mathscr{B}(\vec{u}_n)$.* By I.H.,

$$\mathfrak{F}_{\mathscr{B}}(a_1, \ldots, a_n) = \{\langle u_1, \ldots, u_n\rangle \in a_1 \times \cdots \times a_n : \mathscr{B}^{\mathbb{L}_N}(\vec{u}_n)\}$$

is in $\mathbb{L}_N$. Since $(\neg\mathscr{B})^{\mathbb{L}_N}$ is $\neg(\mathscr{B}^{\mathbb{L}_N})$,

$$\mathfrak{F}_{\mathscr{A}}(a_1, \ldots, a_n) = a_1 \times \cdots \times a_n - \mathfrak{F}_{\mathscr{B}}(a_1, \ldots, a_n)$$

and the result follows from VI.9.5 and VI.9.8.

*Case $\mathscr{A}(\vec{u}_n)$ is $\mathscr{B}(\vec{u}_n) \vee \mathscr{C}(\vec{u}_m)$, say, with $m \le n$.* By I.H.,

$$\mathfrak{F}_{\mathscr{B}}(a_1, \ldots, a_n) = \{\langle u_1, \ldots, u_n\rangle \in a_1 \times \cdots \times a_n : \mathscr{B}^{\mathbb{L}_N}(\vec{u}_n)\}$$

and

$$\mathfrak{F}_{\mathscr{C}}(a_1, \ldots, a_m) = \{\langle u_1, \ldots, u_m\rangle \in a_1 \times \cdots \times a_m : \mathscr{C}^{\mathbb{L}_N}(\vec{u}_m)\}$$

are in $\mathbb{L}_N$. Since $(\mathscr{B} \vee \mathscr{C})^{\mathbb{L}_N}$ is $(\mathscr{B}^{\mathbb{L}_N}) \vee (\mathscr{C}^{\mathbb{L}_N})$,

$$\mathfrak{F}_{\mathscr{A}}(a_1, \ldots, a_n) = \mathfrak{F}_{\mathscr{B}}(a_1, \ldots, a_n) \cup \mathfrak{F}_{\mathscr{C}}(a_1, \ldots, a_m) \times a_{m+1} \times \cdots \times a_n$$

and the result follows from VI.9.5 and VI.9.8 ("$\times\, a_{m+1} \times \cdots \times a_n$" above is absent if $n = m$).

Finally,

*Case $\mathscr{A}(\vec{u}_n)$ is $(\exists y)\mathscr{B}(\vec{u}_n, y)$.* By I.H.,

$$\begin{aligned}&\mathfrak{F}_{\mathscr{B}}(a_1, \ldots, a_n, b)\\ &\qquad = \{\langle u_1, \ldots, u_n, y\rangle \in a_1 \times \cdots \times a_n \times b : \mathscr{B}^{\mathbb{L}_N}(\vec{u}_n, y)\}\end{aligned} \tag{1}$$

is in $\mathbb{L}_N$ for any $N$-constructible $a_1, \ldots, a_n, b$. As we want to show that

$$\begin{aligned}
&\mathfrak{F}_{\mathscr{A}}(a_1, \ldots, a_n)\\
&\quad = \left\{\langle u_1, \ldots, u_n\rangle \in a_1 \times \cdots \times a_n : \left[(\exists y).\mathscr{B}(\vec{u}_n, y)\right]^{\mathbb{L}_N}\right\}\\
&\quad = \left\{\langle u_1, \ldots, u_n\rangle \in a_1 \times \cdots \times a_n : (\exists y \in \mathbb{L}_N).\mathscr{B}^{\mathbb{L}_N}(\vec{u}_n, y)\right\}
\end{aligned}$$

is in $\mathbb{L}_N$, it suffices to prove there is an $N$-constructible set $b$ for which (3) below holds. Then

$$\mathfrak{F}_{\mathscr{A}}(a_1, \ldots, a_n) = \operatorname{dom}(\mathfrak{F}_{\mathscr{B}}(a_1, \ldots, a_n, b)) \tag{2}$$

and we are done by VI.9.9.

Now consider

$$\begin{aligned}
&\big(\forall\langle\vec{u}_n\rangle \in a_1 \times \cdots \times a_n\big)(\exists y \in b)\Big(y \in \mathbb{L}_N \wedge \big[\mathscr{B}^{\mathbb{L}_N}(\vec{u}_n, y)\\
&\qquad\qquad \vee\, y = \emptyset \wedge \neg(\exists z \in \mathbb{L}_N).\mathscr{B}^{\mathbb{L}_N}(\vec{u}_n, z)\big]\Big)
\end{aligned} \tag{3}$$

We prove (3) as a consequence of

$$\begin{aligned}
&\big(\forall\langle\vec{u}_n\rangle \in a_1 \times \cdots \times a_n\big)(\exists y)\Big(y \in \mathbb{L}_N \wedge \big[\mathscr{B}^{\mathbb{L}_N}(\vec{u}_n, y)\\
&\qquad\qquad \vee\, y = \emptyset \wedge \neg(\exists z \in \mathbb{L}_N).\mathscr{B}^{\mathbb{L}_N}(\vec{u}_n, z)\big]\Big)
\end{aligned} \tag{4}$$

Let us prove (4). Let $\langle\vec{u}_n\rangle \in a_1 \times \cdots \times a_n$.

*Case 1.* $(\exists y)\big(y \in \mathbb{L}_N \wedge \mathscr{B}^{\mathbb{L}_N}(\vec{u}_n, y)\big)$. Then (4) follows by tautological implication and $\exists$-monotonicity.

*Case 2.* $\neg(\exists z)\big(z \in \mathbb{L}_N \wedge \mathscr{B}^{\mathbb{L}_N}(\vec{u}_n, z)\big)$. Note that $\emptyset$ is constructible: If $N \neq \emptyset$, then $\emptyset = p - p$,[†] where $p \in N$ ($p$ is, of course, in $\mathbb{L}_N$). If $N = \emptyset$, then $\emptyset = F_0$. Thus $\emptyset \in \mathbb{L}_N \wedge \emptyset = \emptyset \wedge \neg(\exists z \in \mathbb{L}_N).\mathscr{B}^{\mathbb{L}_N}(\vec{u}_n, z)$ is provable; hence so is $(\exists y)\big(y \in \mathbb{L}_N \wedge y = \emptyset \wedge \neg(\exists z \in \mathbb{L}_N).\mathscr{B}^{\mathbb{L}_N}(\vec{u}_n, z)\big)$ by the substitution axiom. Now (4) follows once more by tautological implication and $\exists$-monotonicity.

By collection,[‡] there is a set $A$ (new constant) such that

$$\begin{aligned}
&\big(\forall\langle\vec{u}_n\rangle \in a_1 \times \cdots \times a_n\big)(\exists y \in A)\Big(y \in \mathbb{L}_N \wedge \big[\mathscr{B}^{\mathbb{L}_N}(\vec{u}_n, y)\\
&\qquad\qquad \vee\, y = \emptyset \wedge \neg(\exists z \in \mathbb{L}_N).\mathscr{B}^{\mathbb{L}_N}(\vec{u}_n, z)\big]\Big)
\end{aligned}$$

[†] Recall that the formal difference makes sense on atoms. Cf. III.4.16.

[‡] "$y \in \mathbb{L}_N$" is, of course, the set theory formula "$(\exists\alpha)y = F_\alpha$" – see Definition VI.9.2.

Take then for $b$ (new constant) any $N$-constructible set satisfying $A \cap \mathbb{L}_N \subseteq b$ (by VI.9.7). We can now verify (2):

$$\begin{aligned}
&\langle \vec{u}_n \rangle \in \mathfrak{F}_{\mathscr{A}}(a_1, \ldots, a_n)\\
\leftrightarrow\\
&\langle \vec{u}_n \rangle \in a_1 \times \cdots \times a_n \wedge (\exists y \in \mathbb{L}_N).\mathscr{B}^{\mathbb{L}_N}(\vec{u}_n, y)\\
\leftrightarrow &\Big\langle \rightarrow\text{: by (4)}\rightarrow\text{(3); }\leftarrow\text{: by (3) and VI.9.3, since } b \in \mathbb{L}_N \Big\rangle\\
&\langle \vec{u}_n \rangle \in a_1 \times \cdots \times a_n \wedge (\exists y \in b).\mathscr{B}^{\mathbb{L}_N}(\vec{u}_n, y)\\
\leftrightarrow\\
&(\exists y)\Big( y \in b \wedge \langle \vec{u}_n \rangle \in a_1 \times \cdots \times a_n \wedge \mathscr{B}^{\mathbb{L}_N}(\vec{u}_n, y)\Big)\\
\leftrightarrow\\
&\langle \vec{u}_n \rangle \in \operatorname{dom}\big(\mathfrak{F}_{\mathscr{B}}(a_1, \ldots, a_n, b)\big)
\end{aligned}$$

□

**VI.9.13 Theorem.** $\mathfrak{J} = (L_{\text{Set}}, \text{ZF}, \mathbb{L}_N)$ *is a formal model of* ZFC.

N.B. Actually, $L_{\text{Set}}$ and ZF contain $N$ and $f$ and their axiom (VI.9.2).

*Proof. The proof is in* ZF. First off, $\mathbb{L}_N \neq \emptyset$. Indeed, we have shown in the course of the previous proof that $\emptyset \in \mathbb{L}_N$. We verify now the ZFC axioms.

(1) Extensionality holds in $\mathbb{L}_N$ by VI.9.4 and VI.8.10.

(2) For the axiom

$$U(b) \rightarrow \neg(\exists x) x \in b$$

we want

$$b \in \mathbb{L}_N \rightarrow U(b) \rightarrow \neg(\exists x \in \mathbb{L}_N) x \in b$$

which follows from the ZF version preceding it.

(3) The axiom of separation says that

$$A(\vec{u}_{i-1}, a, u_{i+1}, \ldots, u_n) = \{u_i : u_i \in a \wedge \mathscr{P}(\vec{u}_n)\}$$

is a set (parametrized by the free variables $a$ and $u_j$, $1 \leq j < i \vee i < j \leq n$) for any formula $\mathscr{P}$. The relativized version asserts that

$$A^{\mathbb{L}_N}(\vec{u}_{i-1}, a, u_{i+1}, \ldots, u_n) = \{u_i \in \mathbb{L}_N : u_i \in a \wedge \mathscr{P}^{\mathbb{L}_N}(\vec{u}_n)\} \tag{$i$}$$

is constructible from $N$ whenever $a$ and $u_j$, $1 \leq j < i \vee i < j \leq n$, are (cf. VI.8.13).

So, we let $a$ and $u_j$, $1 \leq j < i \vee i < j \leq n$, be in $\mathbb{L}_N$ and prove that $A^{\mathbb{L}_N}(\vec{u}_{i-1}, a, u_{i+1}, \ldots, u_n) \in \mathbb{L}_N$. By transitivity of $\mathbb{L}_N$, $(i)$ simplifies to

$$A^{\mathbb{L}_N}(\vec{u}_{i-1}, a, u_{i+1}, \ldots, u_n) = \{u_i : u_i \in a \wedge \mathscr{P}^{\mathbb{L}_N}(\vec{u}_n)\} \tag{$i'$}$$

Now, by VI.9.5, VI.9.12, and VI.9.8,

$$\begin{aligned}&\mathfrak{F}_{\mathscr{P}}(\{u_1\},\ldots,\{u_{i-1}\},a,\{u_{i+1}\},\ldots,\{u_n\})\\ &\quad=\{\langle\vec{x}_n\rangle\in\{u_1\}\times\cdots\times\{u_{i-1}\}\times a\times\{u_{i+1}\}\times\cdots\times\{u_n\}:\mathscr{P}^{\mathbb{L}_N}(\vec{x}_n)\}\end{aligned}$$

is constructible. Hence

$$A^{\mathbb{L}_N}(\vec{u}_{i-1},a,u_{i+1},\ldots,u_n)=\begin{cases}\mathrm{ran}\,\underbrace{\mathrm{dom}\cdots\mathrm{dom}}_{n-i\text{ terms}}(\mathfrak{F}_{\mathscr{P}}) & \text{if } i>1\\ \underbrace{\mathrm{dom}\cdots\mathrm{dom}}_{n-1\text{ terms}}(\mathfrak{F}_{\mathscr{P}}) & \text{otherwise}\end{cases}$$

which is in $\mathbb{L}_N$, considering that $\mathrm{ran}(x)=\mathrm{dom}(\mathfrak{F}_{10}(x))$.

(4) Existence of the set of urelements: $\{x : U(x)\}$ is a set. We want to prove (cf. VI.8.13)

$$\{x\in\mathbb{L}_N : U(x)\}\in\mathbb{L}_N$$

In view of the already noted $sp(F_\alpha)\subseteq N$ and $N\subseteq\mathbb{L}_N$ ($N=\{F_\alpha:\alpha<\|N\|\}$), the above translates to $N\in\mathbb{L}_N$. Now, since $N\subseteq\mathbb{L}_N$ (and $N$ is a set), there is, by VI.9.7, an $N$-constructible set $A$ such that $N\subseteq A$. But then $N=\{x\in A:U(x)\}$; hence it is constructible by $\mathbb{L}_N$-separation ((3) above).

(5) The pairing axiom: For any atoms or sets $a$ and $b$, there is a set $c$ such that $a\in c$ and $b\in c$. Thus, we want (by VI.8.13) to show that $\{a,b\}$ is defined in $\mathbb{L}_N$. Since $\{a,b\}^{\mathbb{L}_N}=\{a,b\}$, this follows from VI.9.5.

(6) The union axiom states, essentially, that if $A$ is a set, then $\bigcup A$ is a set. For the $\mathbb{L}_N$ version we need $\bigcup$ to be defined in $\mathbb{L}_N$ (again by VI.8.13). Since (by VI.8.16 and VI.9.4) $\bigcup$ is absolute for $\mathbb{L}_N$, we need to show that $\mathbb{L}_N$ is $\bigcup$-closed. For $A\in\mathbb{L}_N$, $\bigcup A=\{x:(\exists y\in A)x\in y\}\subseteq\mathbb{L}_N$ by VI.9.3. Hence $\bigcup A\subseteq b\in\mathbb{L}_N$ for some $b$ (by VI.9.7), and $\bigcup A\in\mathbb{L}_N$ by $\mathbb{L}_N$-separation.

(7) Foundation holds in $\mathbb{L}_N$ by VI.8.11.

(8) Collection says that for any set $A$ and formula $\mathscr{P}[x,y]$,

$$(\forall x\in A)(\exists y)\mathscr{P}[x,y]\to(\exists z)(\forall x\in A)(\exists y\in z)\mathscr{P}[x,y]$$

Letting $A\in\mathbb{L}_N$, we want to prove the relativized version

$$\begin{aligned}&(\forall x\in A)(\exists y\in\mathbb{L}_N)\mathscr{P}^{\mathbb{L}_N}[x,y]\\ &\qquad\to(\exists z\in\mathbb{L}_N)(\forall x\in A)(\exists y\in z)\mathscr{P}^{\mathbb{L}_N}[x,y]\end{aligned}\tag{$iii$}$$

So assume the hypothesis of $(iii)$, i.e.,

$$(\forall x\in A)(\exists y)\big[(\exists\alpha)y=F_\alpha\wedge\mathscr{P}^{\mathbb{L}_N}[x,y]\big]$$

By collection (in ZF), there is a set $w$ (new constant) such that

$$(\forall x \in A)(\exists y \in w)\big[(\exists \alpha) y = F_\alpha \wedge \mathscr{P}^{\mathbb{L}_N}[x, y]\big] \tag{$iv$}$$

By VI.9.7 there is a set $s \in \mathbb{L}_N$ (new constant) such that $w \cap \mathbb{L}_N \subseteq s$. Let

$$z = \Big\{ y \in s : (\exists x \in A) \mathscr{P}^{\mathbb{L}_N}[x, y] \Big\} \tag{$v$}$$

By $\mathbb{L}_N$-separation, $z \in \mathbb{L}_N$. Moreover, this $z$ works to establish the conclusion of $(iii)$. Indeed, $\underline{\text{let } x \in A}$. By $(iv)$ we derive

$$(\exists y)(\exists \alpha)\big[y \in w \wedge y = F_\alpha \wedge \mathscr{P}^{\mathbb{L}_N}[x, y]\big]$$

since without loss of generality $\alpha$ is not free in $\mathscr{P}$. Introduce now new constants $Y$ and $\beta$ and the assumption

$$Y \in w \wedge Y = F_\beta \wedge \mathscr{P}^{\mathbb{L}_N}[x, Y]$$

The first two conjuncts imply that $Y \in s$ hence, by $(v)$, $Y \in z$. Thus,

$$Y \in z \wedge \mathscr{P}^{\mathbb{L}_N}[x, Y]$$

hence $(\exists y)\big(y \in z \wedge \mathscr{P}^{\mathbb{L}_N}[x, y]\big)$ from which generalization and the underlined assumption (deduction theorem used) yield

$$(\forall x \in A)(\exists y \in z) \mathscr{P}^{\mathbb{L}_N}[x, y]$$

The right hand side of $(iii)$ is now obtained by the substitution axiom and modus ponens.

(9) The power set axiom says that for any set $A$, $\{x : x \subseteq A\}$ is a set too. For the $\mathbb{L}_N$ version we want $\mathbf{P}(A)$ to be defined in $\mathbb{L}_N$. Now $\mathbf{P}^{\mathbb{L}_N}(A) = \mathbf{P}(A) \cap \mathbb{L}_N$ (Exercise VI.60), a set by the power set axiom and separation in ZF. Since $\mathbf{P}(A) \cap \mathbb{L}_N \subseteq \mathbb{L}_N$, $\mathbf{P}^{\mathbb{L}_N}(A)$ is constructible by VI.9.7 and $\mathbb{L}_N$-separation.

(10) The relativization of the axiom of infinity, essentially, says $\omega^{\mathbb{L}_N} \in \mathbb{L}_N$. Thus, if we can prove that $\omega \in \mathbb{L}_N$, then we will be done, since $\omega^{\mathbb{L}_N} = \omega$ will follow (by remarks in VI.8.18). We will prove a bit more for convenience, namely,

$$\mathrm{On} \subseteq \mathbb{L}_N$$

So take as induction hypothesis that

$$(\forall \beta < \alpha) \beta \in \mathbb{L}_N$$

Proceeding now exactly as in the proof of VI.9.7, there is a *limit ordinal* $\gamma$ such that $\alpha \subseteq F_\gamma$. Let $A = \{\sigma : \sigma \in F_\gamma\}$ and $\tau \in \sigma \in A$. First, $\sigma = F_\rho$ for $\rho < \gamma$, by VI.9.3. Hence, $\tau \in \sigma \subseteq F_\gamma$, since $\mathrm{Lim}(\gamma)$ (see VI.9.2). Thus, $A$ is transitive;

hence $A \in \mathrm{On}$. Furthermore, $A \in \mathbb{L}_N$ by $\mathbb{L}_N$-separation.[†] Clearly, $\alpha \subseteq A$. If $\alpha = A$, then $\alpha \in \mathbb{L}_N$. If $\alpha \in A$, then again $\alpha \in \mathbb{L}_N$ by transitivity of $\mathbb{L}_N$.

(11) The axiom of choice, relativized in $\mathbb{L}_N$, says that if $A$ is a (constructible) set of nonempty constructible sets, then there is a choice function $c$ with $\mathrm{dom}(c) = A$ such that $(\forall x \in A)c(x) \in x$. To prove this just take

$$c(x) = F_{\min\{\alpha\,:\, F_\alpha \in x\}} \qquad \square$$

**VI.9.14 Corollary.** *If* ZF *is consistent, then so is* ZFC.

*Proof.* By our previous construction and the results of Section I.7. Note that the auxiliary constant metatheorem is being invoked, since neither the hypothesis nor the conclusion refers to the new constants $N$ and $f$ introduced as per the footnote on p. 396. c.f. p. 75. □

Gödel also showed that the generalized continuum hypothesis is true in $\mathbb{L}_N$, and hence consistent with ZF *and* AC (see VII.7.25).

We conclude the section by briefly exploring some easy consequences of absoluteness considerations, mostly stated as exercises.

**VI.9.15 Exercise.** Prove that all Gödel operations, including the three derived ones, are absolute for transitive models of ZF. Are they absolute for any other classes? □

**VI.9.16 Exercise.** Prove that the function $\lambda\alpha.F_\alpha$ is absolute for $\mathbb{L}_N$ when the constants $N$, $f$ are interpreted as themselves.

*Hint.* This follows from VI.9.15 and techniques in Section VI.8 (cf. in particular VI.8.20 and VI.8.26). Note that $f : \mathrm{dom}(f) \to N$ is in $\mathbb{L}_N$. This is so by $\mathrm{dom}(f) \in \mathrm{On} \subseteq \mathbb{L}_N$, $f \subseteq \mathrm{dom}(f) \times N$, and closure of $\mathbb{L}_N$ under $\times$ (now apply $\mathbb{L}_N$-separation). □

The *axiom of constructibility* says that all objects are in $\mathbb{L}_N$, or all objects are constructible.[‡] Formally then it is

$$(\forall x)(\exists\alpha)x = F_\alpha \qquad (\mathbb{V} = \mathbb{L})$$

It denoted by "$\boldsymbol{V} = \boldsymbol{L}$" or "$\mathbb{V} = \mathbb{L}$" depending on typeface preference.

[†] $A = \{\sigma : \sigma \in F_\gamma\} = \{x \in F_\gamma : x \text{ is an ordinal}\}$. See VI.8.16.

[‡] In atomless approaches to ZF, an object has to be a set.

It must be noted however that the formula displayed generically as $(\mathbb{V} = \mathbb{L})$ depends on the choice of $N$ used in the construction of the function $\alpha \mapsto F_\alpha$, and hence of $\mathbb{L}_N$. What $N$ we have in mind in a particular argument should be clear from the context, if the particular choice affects results claimed. Set theorists do not believe that the axiom of constructibility is (really) true, but they find it interesting as a "temporary" axiom. For one thing, *it is harmless*:

**VI.9.17 Theorem.** *If* ZF *is consistent, then so is* $\mathrm{ZF} + (\mathbb{V} = \mathbb{L})$*. Indeed,* $\mathbb{V} = \mathbb{L}$ *is true in* $\mathfrak{J} = (L_{\mathrm{Set}}, \mathrm{ZF}, \mathbb{L}_N)$*, where* ZF *is extended as in VI.9.2.*

*Proof.* $(\mathbb{V} = \mathbb{L})^{\mathbb{L}_N}$ is $(\forall x \in \mathbb{L}_N)(\exists \alpha \in \mathbb{L}_N)(x = F_\alpha)^{\mathbb{L}_N}$; hence, by VI.9.16 and $\mathrm{On} \subseteq \mathbb{L}_N$, one needs to prove

$$(\forall x \in \mathbb{L}_N)(\exists \alpha) x = F_\alpha$$

This is precisely VI.9.2. □

For another thing, *it simplifies the relativization of arguments to* $\mathbb{L}_N$: Suppose that we want to prove (having set $N^{\mathbb{L}_N} = N$ and $f^{\mathbb{L}_N} = f$)

$$\vdash_{\mathrm{ZF}} \mathscr{A}^{\mathbb{L}_N} \tag{1}$$

for some sentence $\mathscr{A}$ of the extended $L_{\mathrm{Set}}$. Suppose that we prove

$$\vdash_{\mathrm{ZF}+(\mathbb{V}=\mathbb{L})} \mathscr{A} \tag{2}$$

instead, which results in a proof of (by the deduction theorem)

$$\vdash_{\mathrm{ZF}} \mathbb{V} = \mathbb{L} \to \mathscr{A} \tag{3}$$

Since $\mathfrak{J}$ is a formal model of ZF (the $N$, $f$-axiom is true in $\mathfrak{J}$), (3) implies (cf. I.7.9)

$$\models_{\mathfrak{J}} (\mathbb{V} = \mathbb{L}) \to \mathscr{A}$$

But $\models_{\mathfrak{J}} (\mathbb{V} = \mathbb{L})$ by VI.9.17; thus $\models_{\mathfrak{J}} \mathscr{A}$; that is, we have derived (1).

Conversely, suppose we have proved (1). We show that (2) follows. To this end we show by induction on formulas that

$$\mathbb{V} = \mathbb{L} \vdash \mathscr{A} \leftrightarrow \mathscr{A}^{\mathbb{L}_N} \tag{4}$$

We just check the interesting case where $\mathscr{A} \equiv (\exists x)\mathscr{B}$. Now $\mathscr{A}^{\mathbb{L}_N} \equiv (\exists x)\big((\exists \alpha)\, x = F_\alpha \wedge \mathscr{B}^{\mathbb{L}_N}\big)$, while

$$\mathbb{V} = \mathbb{L} \vdash (\exists x)\big((\exists \alpha) x = F_\alpha \wedge \mathscr{B}^{\mathbb{L}_N}\big) \leftrightarrow (\exists x)\big((\exists \alpha) x = F_\alpha \wedge \mathscr{B}\big) \tag{5}$$

by the I.H. But $\mathbb{V} = \mathbb{L} \vdash \big((\exists\alpha)x = F_\alpha \wedge \mathscr{B}\big) \leftrightarrow \mathscr{B}$, since the hypothesis – $(\forall x)(\exists\alpha)x = F_\alpha$ – implies $(\exists\alpha)x = F_\alpha$. This and (5) yield (4) via the Leibniz rule.

Thus, if we have (1), then we also have $\vdash_{\mathrm{ZF}+(\mathbb{V}=\mathbb{L})} \mathscr{A}^{\mathbb{L}_N}$, and hence (2), by (4).

The moral, in plain English, is:

**VI.9.18 Remark.** To prove in ZF a sentence $\mathscr{A}$ relativized to $\mathbb{L}_N$, add the axiom of constructibility and prove instead the unrelativized sentence $\mathscr{A}$. □

**VI.9.19 Exercise.** Prove that $\mathbb{L}_N$ is the $\subseteq$-smallest proper class (formal) model of ZF among those that contain $N$. In particular, $\mathbb{L}$ (cf. VI.9.2) is the $\subseteq$-smallest proper class (formal) model of ZF.

*Hint.* Indeed, let $\mathbb{M}$ be a proper class model of ZF where $N \in \mathbb{M}$. First show that $\mathrm{On} \subseteq \mathbb{M}$: Let $\alpha \in \mathrm{On}$. Look for a $\beta \in \mathbb{M}$ such that $\alpha \leq \beta$. For example, as $\mathbb{M}$ is not a set, pick an $x \in \mathbb{M} - N \cup V_N(\alpha)$. By VI.8.25, $\rho(x) \in \mathbb{M}$. This is a good enough $\beta$. Conclude by computing $\mathbb{L}_N^{\mathbb{M}}$. Towards this you will need that $\lambda\alpha.F_\alpha$ is absolute for $\mathbb{M}$, in particular, that $f$ of VI.9.2 is in $\mathbb{M}$. The latter is argued as in VI.9.16, using the absoluteness of $\times$ (cf. VI.8.16). □

**VI.9.20 Remark.** Our discussion has focused so far on "large" models $\mathbb{M}$, i.e., proper class models. These have the advantage of containing all the ordinals. One is also interested in "small" transitive $(U, \in)$-models of ZF, $M$, where $M$ is a set. We can easily adjust the constant $N$ of p. 396 so that the related assumption is

$$\neg U(N) \wedge (\forall z \in N)U(z) \wedge f \text{ is a 1-1 function} \wedge \mathrm{dom}(f) \subseteq \omega \wedge \mathrm{ran}(f) = N$$

Since $M$ satisfies infinity, the constant $\omega$ is absolute for $M$. The additional assumption that $N \in M$ will then yield that $\lambda\alpha.F_\alpha$ is absolute for $M$ (cf. VI.8.19). □

## VI.10. Arithmetic on the Ordinals

Infinite sequences extend the notion of an $n$-tuple, while transfinite sequences extend the notion of an infinite sequence. Just as in the case of finite sequences (V.1.28–V.1.29), where we can juxtapose or concatenate them to obtain a sequence whose length is the sum of the lengths of the originals (V.1.30), we are able to do that with arbitrarily "long" WO sets, in particular with canonical WO sets, i.e., ordinals.

For example, on concatenating $\alpha$ and $\beta$ in that order ($\alpha * \beta$) we expect, informally speaking, to end up with the sequence

$$\{0, 1, 2, \ldots, \alpha, \alpha + 1, \ldots\} \tag{1}$$

of length, intuitively, $\alpha + \beta$ , as is the case when $\alpha$, $\beta$ are natural numbers. We would also like to be able to iterate concatenation, for example concatenating $\alpha$ with itself "$\beta$ times", to obtain

$$\underbrace{\alpha * \alpha * \cdots * \alpha}_{\text{a sequence of } \beta \text{ copies of } \alpha} \tag{2}$$

of length, intuitively, $\alpha \cdot \beta$.

Let us first make addition of ordinals precise by extending the recursive definition of addition over $\omega$ (V.1.22).[†]

**VI.10.1 Definition (Addition of Ordinals).** The unique function $A(\alpha, \beta)$ given by the recursion below will be denoted by "$\alpha + \beta$":

$$\begin{aligned} A(\alpha, 0) &= \alpha \\ A(\alpha, \beta + 1) &= A(\alpha, \beta) + 1 \\ \text{for } \mathrm{Lim}(\beta), \quad A(\alpha, \beta) &= \sup\{A(\alpha, \gamma) : \gamma < \beta\} \end{aligned} \qquad \square$$

In the definition we use "+" with potentially two different meanings: The new meaning is given in the definition. The old meaning is in the use of "+1" to mean ordinal successor. It will turn out that the two meanings are consistent.

**VI.10.2 Proposition.** *$\lambda\beta.\alpha + \beta$ is normal for any $\alpha$.*

*Proof.* By VI.5.38 and the weak continuity of $\lambda\beta.\alpha + \beta$, we only need to show that $\alpha + \beta < \alpha + (\beta + 1)$. But, by VI.10.1, this translates to

$$\begin{aligned} \alpha + \beta &< (\alpha + \beta) + 1 \\ &= (\alpha + \beta) \cup \{\alpha + \beta\} \end{aligned} \qquad \square$$

**VI.10.3 Corollary.** *If* $\mathrm{Lim}(\beta)$*, then* $\mathrm{Lim}(\alpha + \beta)$.

*Proof.* By VI.5.40. □

We next prove the analogue of V.1.25, which shows that Definition VI.10.1 indeed captures the intuitive meaning of (1) in the preamble to this section.

[†] All the results in this section are due to Cantor.

**VI.10.4 Theorem.** $\alpha + \beta = \alpha \cup \{\alpha + \gamma : \gamma < \beta\}$.

*Proof.* We do induction on $\beta$. The basis and the case $\beta + 1$ are handled exactly as in V.1.25.

So, let $\mathrm{Lim}(\beta)$, and assume (I.H.) that whenever $\gamma < \beta$,

$$\alpha + \gamma = \alpha \cup \{\alpha + \lambda : \lambda < \gamma\} \tag{1}$$

Now $\beta > 0$; hence $\alpha < \alpha + \beta$, using VI.10.2 (since $\alpha + 0 = \alpha$ by VI.10.1); thus $\alpha \subset \alpha + \beta$. Moreover, by VI.10.2 again, $\alpha + \gamma < \alpha + \beta$, that is, $\alpha + \gamma \in \alpha + \beta$. Thus

$$\alpha + \beta \supseteq \alpha \cup \{\alpha + \rho : \rho < \beta\} \tag{2}$$

Let now $\delta \in \alpha + \beta = \bigcup\{\alpha + \tau : \tau < \beta\}$. Thus, $\delta \in \alpha + \tau$ for some $\tau < \beta$, and, by (1), $\delta \in \alpha$ or $\delta = \alpha + \lambda$ for some $\lambda < \tau$. Thus $\delta$ is in the right hand side of (2), and we get the converse inclusion of (2). □

**VI.10.5 Remark (On Notation).** (1) We re-examine the notation $\alpha + 1$, which we have adopted to mean $\alpha \cup \{\alpha\}$. Using the theorem above and thinking of "+" here as addition rather than successor, we get

$$\begin{aligned} \alpha + 1 &= \alpha \cup \{\alpha + \gamma : \gamma < 1\} \\ &= \alpha \cup \{\alpha + 0\} \\ &= \alpha \cup \{\alpha\} \qquad \text{by VI.10.1} \end{aligned}$$

Thus the new notation $\alpha + \beta$ and the old $\alpha + 1$ mean the same thing when $\beta = 1$.

(2) Often, the notation $\dotplus$ is used instead of $+$ for ordinal addition, $+$ being reserved for cardinal addition. For the addition of cardinals we will use $+_c$. We use $\dotplus$ for something else (see below). □

We next relate the ordinal of a WO set obtained by *concatenation* of two WO sets to those of the originals. As intuition dictates, it will be the sum of the two original ordinals. Thus the length of the concatenation of a WO set is the sum of the lengths of its two components, as it should be.

**VI.10.6 Definition.**

(i) The *disjoint union* of sets $X$ and $Y$ is the set $\{0\} \times X \cup \{1\} \times Y$, denoted $X \dotplus Y$.
(ii) If $(X_\beta)_{\beta \in \alpha}$ is an $\alpha$-sequence of sets, then their *ordered disjoint sum* is $\bigcup_{\beta \in \alpha}(\{\beta\} \times X_\beta)$ and is denoted by $\sum_{\beta \in \alpha} X_\beta$. □

Clearly, $X_0 \dotplus X_1 = \sum_{\beta\in 2} X_\beta$. Note that $X \dotplus Y \neq Y \dotplus X$ in general (e.g., take $X = \{0\}$ and $Y = \{1\}$.)

**VI.10.7 Definition.**

(i) Let $(X, <_1)$ and $(Y, <_2)$ be two WO sets. Then $<_*$ on $X \dotplus Y$ is defined *lexicographically*, i.e.,

$$\begin{aligned} \langle i, x\rangle <_* \langle j, y\rangle \quad \text{iff} \quad & i < j \vee \\ & i = j = 0 \wedge x <_1 y \vee \\ & i = j = 1 \wedge x <_2 y \end{aligned}$$

(ii) Let $(X_\beta, <_\beta)$ be a WO set for all $\beta \in \alpha$. Then $<_\Sigma$ on $\sum_{\beta\in\alpha} X_\beta$ is defined lexicographically by

$$\begin{aligned} \langle \beta, x\rangle <_\Sigma \langle \gamma, y\rangle \quad \text{iff} \quad & \beta < \gamma \vee \\ & \beta = \gamma \wedge x <_\beta y \end{aligned}$$ □

**VI.10.8 Proposition.** *$<_*$ and $<_\Sigma$ of* VI.10.7 *are indeed well-orderings.*

*Proof.* That they are linear orders is straightforward. Moreover, in either case, any nonempty set of pairs $\langle \beta, x\rangle$ has a minimum: Locate the ones with $<$-minimum $\beta$ among such pairs; in this set locate the pair with $<_\beta$-minimum $x$ (in $X_\beta$). □

**VI.10.9 Definition (Concatenation of WO Sets).** Given WO sets $(X_\beta, <_\beta)$ for all $\beta \in \alpha$, their concatenation $\mathrm{cat}_{\beta\in\alpha}(X_\beta, <_\beta)$ is the WO set $(\sum_{\beta\in\alpha} X_\beta, <_\Sigma)$.

In particular, when $\alpha = 2$ we write also $(X_0, <_0) * (X_1, <_1)$ for the concatenation, and we denote $<_\Sigma$ by $<_*$ in this case. □

The following theorem shows that the definition of addition of ordinals is appropriate.

**VI.10.10 Theorem.** *If $\|(X_0, <_0)\| = \alpha$ and $\|(X_1, <_1)\| = \beta$, then $\|(X_0, <_0) * (X_1, <_1)\| = \alpha + \beta$.*

*Proof.* Let

$$\alpha \overset{f}{\cong} X_0 \tag{1}$$

and

$$\beta \overset{g}{\cong} X_1 \tag{2}$$

where we have omitted the relevant orders to the left ($\in$) and right ($<_i$, $i = 0, 1$) of $\cong$ for simplicity of notation.

Let $\tilde{f} = \{\langle\gamma, \langle 0, f(\gamma)\rangle\rangle : \gamma \in \alpha\}$ and $\tilde{g} = \{\langle\alpha + \gamma, \langle 1, g(\gamma)\rangle\rangle : \gamma \in \beta\}$. Since $\alpha \leq \alpha + \gamma$ (with the "=" when $\gamma = 0$), we have $\mathrm{dom}(\tilde{f}) \cap \mathrm{dom}(\tilde{g}) = \emptyset$; hence $H = \tilde{f} \cup \tilde{g}$ is a total function on $\mathrm{dom}(\tilde{f}) \cup \mathrm{dom}(\tilde{g})$, that is, on $\alpha + \beta$, by VI.10.4. $H$ is onto $X_0 \dot{+} X_1$ since $\tilde{f}$ and $\tilde{g}$ are onto $\{0\} \times X_0$ and $\{1\} \times X_1$ respectively, by (1) and (2).

By (1) and (2), and Definition VI.10.7, $H$ is order-preserving and hence an isomorphism between $\alpha + \beta$ and $(X_0 \dot{+} X_1, <_*)$. □

**VI.10.11 Proposition (Some Properties of Ordinal Addition).**

$(i)$ $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$
$(ii)$ $\alpha < \beta \rightarrow \alpha + \gamma \leq \beta + \gamma$
$(iii)$ $\alpha < \beta \leftrightarrow \gamma + \alpha < \gamma + \beta$
$(iv)$ $0 + \alpha = \alpha$
$(v)$ $\alpha < \beta \leftrightarrow (\exists\gamma > 0)\alpha + \gamma = \beta.$

*Proof.* $(i)$: We do induction on $\gamma$. Assume then the claim for all $\lambda < \gamma$. By VI.10.4,

$$\begin{aligned}(\alpha + \beta) + \gamma &= (\alpha + \beta) \cup \{(\alpha + \beta) + \lambda : \lambda < \gamma\} \\ &= (\alpha + \beta) \cup \{\alpha + (\beta + \lambda) : \lambda < \gamma\} && \text{by I.H.} \\ &= \alpha \cup \{\alpha + \delta : \delta < \beta\} \cup \{\alpha + (\beta + \lambda) : \lambda < \gamma\} && \text{by VI.10.4} \quad (1)\end{aligned}$$

Next,

$$\alpha + (\beta + \gamma) = \alpha \cup \{\alpha + \delta : \delta < \beta + \gamma\} \tag{2}$$

Since $\beta + \gamma = \beta \cup \{\beta + \lambda : \lambda < \gamma\}$, $\delta < \beta + \gamma$ is equivalent to (recall that $<$ is $\in$)

$$\delta < \beta \vee (\exists\lambda < \gamma)\delta = \beta + \lambda$$

Thus, (1) and (2) yield the claim.

$(ii)$: We do induction on $\gamma$. The basis follows from the assumption and $\delta + 0 = \delta$ for all $\delta$.

The case $\alpha + (\gamma + 1)$ vs. $\beta + (\gamma + 1)$ follows from $\alpha + \gamma \leq \beta + \gamma$ (I.H.) and VI.5.5.

Let next $\mathrm{Lim}(\gamma)$, and assume that $\alpha + \lambda \leq \beta + \lambda$ for all $\lambda < \gamma$ (I.H.). Then

$$\alpha + \gamma = \sup\{\alpha + \lambda : \lambda < \gamma\} \leq \sup\{\beta + \lambda : \lambda < \gamma\} = \beta + \gamma$$

$(iii)$: From VI.10.2 and trichotomy.

$(iv)$: Assume the claim for all $\beta < \alpha$ (I.H.). By VI.10.4,

$$0 + \alpha = 0 \cup \{0 + \beta : \beta < \alpha\} = \{\beta : \beta < \alpha\} = \alpha$$

$(v)$: The ← follows from $(iii)$ and VI.10.1. For →, let $\alpha < \beta$, hence $\alpha \subset \beta$. Thus the *set difference* $X = \beta - \alpha$ is nonempty and well-ordered by $<$. Let

$$\|(X, <)\| = \gamma \tag{3}$$

Hence $\gamma > 0$ ($X \neq \emptyset$). The function $f$ given by

$$f(\delta) = \begin{cases} \langle 0, \delta \rangle & \text{if } \delta \in \alpha \\ \langle 1, \delta \rangle & \text{if } \delta \in X \end{cases}$$

is trivially an isomorphism

$$\beta \overset{f}{\cong} \{0\} \times \alpha \cup \{1\} \times X$$

Hence $\|(\alpha \dot{+} X, <_*)\| = \beta$. But also $\|(\alpha \dot{+} X, <_*)\| = \alpha + \gamma$ by (3), whence the claim. □

**VI.10.12 Example.** Note that $+$ is not commutative on On. For example,

$$\begin{aligned} 1 + \omega &= \{0\} \cup \{1 + n : n \in \omega\} \\ &= \{0\} \cup \{n + 1 : n \in \omega\} \quad \text{by V.1.24} \\ &= \{n : n \in \omega\} \\ &= \omega \end{aligned}$$

Yet, $\omega < \omega + 1$.

Here is an alternative argument: $\omega + 1$ is a successor, while $\mathrm{Lim}(1 + \omega)$ by VI.5.40, so they cannot be equal. □

We next define multiplication of ordinals by *iterating addition*, as it is done over $\omega$.

**VI.10.13 Definition (Multiplication of Ordinals).** The unique function $M(\alpha, \beta)$ defined by the recursion below will be denoted by "$\alpha \cdot \beta$":

$$\begin{aligned} M(\alpha, 0) &= 0 \\ M(\alpha, \beta + 1) &= M(\alpha, \beta) + \alpha \\ \text{for } \operatorname{Lim}(\beta), \quad M(\alpha, \beta) &= \sup\{M(\alpha, \gamma) : \gamma < \beta\} \end{aligned}$$ □

**VI.10.14 Proposition.** *$\lambda\beta.\alpha \cdot \beta$ is normal for any $\alpha > 0$.*

*Proof.* By VI.5.38 and the weak continuity of $\lambda\beta.\alpha \cdot \beta$, we only need to show that $\alpha \cdot \beta < \alpha \cdot (\beta + 1)$ if $\alpha > 0$. But, by VI.10.13, this translates to

$$\alpha \cdot \beta < (\alpha \cdot \beta) + \alpha$$

which is derivable by VI.10.2. □

**VI.10.15 Corollary.** *If $\alpha > 0$ and $\operatorname{Lim}(\beta)$, then $\operatorname{Lim}(\alpha \cdot \beta)$.*

*Proof.* By VI.5.40. □

**VI.10.16 Theorem.** $\alpha \cdot \beta = \sup\{\alpha \cdot \gamma + \alpha : \gamma < \beta\}$.

*Proof.* We do induction on $\beta$. Let first $\beta = 0$. Then $\alpha \cdot 0 = 0$ by VI.10.13. Also $\sup\{\alpha \cdot \gamma + \alpha : \gamma \in \beta\} = \sup \emptyset = \emptyset$. Done with the basis.

Assume next as I.H.

$$\begin{aligned} \alpha \cdot \beta &= \sup\{\alpha \cdot \gamma + \alpha : \gamma < \beta\} \\ &= \bigcup_{\gamma \in \beta} (\alpha \cdot \gamma + \alpha) \end{aligned} \tag{1}$$

Then, since $\alpha \cdot \beta \subseteq \alpha \cdot \beta + \alpha$ by VI.10.2 ("$=$" corresponds to $\alpha = 0$),

$$\begin{aligned} \alpha \cdot (\beta + 1) &= \alpha \cdot \beta + \alpha \\ &= (\alpha \cdot \beta + \alpha) \cup (\alpha \cdot \beta) \\ &= (\alpha \cdot \beta + \alpha) \cup \bigcup_{\gamma \in \beta} (\alpha \cdot \gamma + \alpha) \quad \text{by (1)} \\ &= \bigcup_{\gamma \in \beta + 1} (\alpha \cdot \gamma + \alpha) \end{aligned}$$

This settles the successor case.

Finally, let $\mathrm{Lim}(\beta)$. Now, by VI.10.13,

$$\begin{aligned}\alpha\cdot\beta &= \bigcup_{\gamma\in\beta}\alpha\cdot\gamma\\ &\subseteq \bigcup_{\gamma\in\beta}(\alpha\cdot\gamma+\alpha) &&\text{since } \alpha\cdot\gamma\subseteq\alpha\cdot\gamma+\alpha\\ &= \bigcup_{\gamma\in\beta}\alpha\cdot(\gamma+1) &&\text{by VI.10.13}\\ &\subseteq \bigcup_{\gamma\in\beta}\alpha\cdot\gamma &&\text{since } \gamma\in\beta\to\gamma+1\in\beta\end{aligned}$$

The I.H. was not needed in this case. □

We next interpret multiplication of ordinals in terms of concatenations of WO sets.

**VI.10.17 Theorem.** *Let $(X_\gamma, <_\gamma)$ be a WO set with order type $\alpha$, for each $\gamma\in\beta$. Then $\|\mathrm{cat}_{\gamma\in\beta}(X_\gamma, <_\gamma)\| = \alpha\cdot\beta$.*

*Proof.* The case $\alpha = 0$ being trivial (each $X_\gamma = \emptyset$), we assume $\alpha > 0$. By Exercise VI.35, it suffices to assume that $X_\gamma = \alpha$ for all $\gamma\in\beta$.

For ease of notation, set $A_\beta = \bigcup_{\gamma<\beta}(\{\gamma\}\times\alpha)$. Take the *induction hypothesis* (on $\beta$) that

$$(\forall\gamma<\beta)\|(A_\gamma, <_\Sigma)\| = \alpha\cdot\gamma \tag{1}$$

Now, since $(A_\beta, <_\Sigma)$ is a WO set, there is a unique isomorphism $\phi_{A_\beta}$ that maps this WO set onto an ordinal. This $\phi$ is given by (see VI.4.32)

$$\begin{aligned}\phi_{A_\beta}(\langle\gamma,\delta\rangle) &= \{\phi_{A_\beta}(\langle\sigma,\tau\rangle) : \langle\sigma,\tau\rangle <_\Sigma \langle\gamma,\delta\rangle\}\\ &= \phi_{A_\beta}\Big[<_\Sigma\big\langle\langle\gamma,\delta\rangle\big\rangle\Big]\end{aligned} \tag{2}$$

for any $\langle\gamma,\delta\rangle\in A_\beta$. Using (1), we now compute the ordinal in (2).

For $\gamma<\beta$ we have

$$\begin{aligned}<_\Sigma\big\langle\langle\gamma,\delta\rangle\big\rangle &= \Big(\bigcup_{\eta<\gamma}(\{\eta\}\times\alpha)\Big)\cup\{\gamma\}\times\delta\\ &\cong \{0\}\times\Big(\bigcup_{\eta<\gamma}(\{\eta\}\times\alpha)\Big)\cup\{1\}\times\delta &&\text{by Exercise VI.36}\\ &= \{0\}\times A_\gamma\cup\{1\}\times\delta\end{aligned}$$

where we have omitted the orders on both sides of the $\cong$. Thus, by the I.H. (1),

$$\begin{aligned}\phi_{A_\beta}(\langle\gamma,\delta\rangle) &= \phi_{A_\beta}\Big[<_\Sigma\big\langle\langle\gamma,\delta\rangle\big\rangle\Big]\\ &= \alpha\cdot\gamma+\delta\end{aligned} \tag{3}$$

We are ready to compute $\|(A_\beta, <_\Sigma)\|$.

For $\gamma < \beta$ and $\delta < \alpha$, we have $\alpha \cdot \gamma + \delta < \alpha \cdot \gamma + \alpha = \alpha \cdot (\gamma + 1)$ by VI.10.2 and VI.10.13. Thus, $\alpha \cdot \gamma + \delta \le \alpha \cdot \beta$ by VI.10.14. We conclude that

$$\phi_{A_\beta}[A_\beta] \subseteq \alpha \cdot \beta \tag{4}$$

Towards promoting (4) to equality, let $\eta \in \alpha \cdot \beta = \bigcup\{\alpha \cdot \gamma + \alpha : \gamma < \beta\}$ by VI.10.16. Thus, $\eta \in \alpha \cdot \gamma + \alpha$ for some $\gamma < \beta$; therefore $\eta \in \alpha \cdot \gamma$ or $\eta = \alpha \cdot \gamma + \delta$ for some $\delta < \alpha$, by VI.10.4. In the latter case, immediately $\eta \in \phi_{A_\beta}[A_\beta]$ by (3). In the former case, $\alpha \cdot \gamma = \alpha \cdot \gamma + 0 \in \phi_{A_\beta}[A_\beta]$ and transitivity of $\phi_{A_\beta}[A_\beta]$ again yield $\eta \in \phi_{A_\beta}[A_\beta]$. Thus (4) is an equality. □

**VI.10.18 Remark.** It is worth noting that $A_\beta = \bigcup_{\gamma<\beta}(\{\gamma\} \times \alpha) = \beta \times \alpha$; thus VI.10.17 shows that

$$(\beta \times \alpha, <_\Sigma) \cong (\alpha \cdot \beta, <)$$

Note the order reversal of the "terms" $\alpha$ and $\beta$. □

**VI.10.19 Proposition (Some Properties of Ordinal Multiplication).**

$(i)$ $0 \cdot \alpha = \alpha \cdot 0 = 0$
$(ii)$ $1 \cdot \alpha = \alpha \cdot 1 = \alpha$
$(iii)$ $\alpha \cdot 2 = \alpha + \alpha$
$(iv)$ $\alpha < \beta \to \alpha \cdot \gamma \le \beta \cdot \gamma$
$(v)$ $\alpha > 0 \to (\alpha \cdot \beta < \alpha \cdot \gamma \leftrightarrow \beta < \gamma)$
$(vi)$ $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$
$(vii)$ $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$
$(viii)$ $\alpha > 1 \wedge \beta > 1 \to \alpha + \beta \le \alpha \cdot \beta$
$(ix)$ $\alpha \ne 0 \ne \beta \to \alpha \cdot \beta \ne 0$.

*Proof.* $(i)$: $0 \cdot \alpha = \bigcup_{\beta<\alpha}(0 \cdot \beta + 0) = 0$, using the I.H. that $0 \cdot \beta = 0$ for $\beta < \alpha$. $\alpha \cdot 0 = 0$ by VI.10.13.

$(ii)$:

$$\begin{aligned} 1 \cdot \alpha &= \bigcup_{\beta<\alpha}(1 \cdot \beta + 1) \\ &= \bigcup_{\beta<\alpha}(\beta + 1) \quad \text{under the obvious I.H.} \\ &= \sup{}^{+}\{\beta : \beta < \alpha\} \\ &= \alpha \end{aligned}$$

On the other hand, $\alpha \cdot 1 = \alpha \cdot 0 + \alpha = \alpha$ (VI.10.13 and VI.10.11$(iv)$).

$(iii)$:

$$\begin{aligned}\alpha \cdot 2 &= \bigcup_{\beta<2}(\alpha \cdot \beta + \alpha)\\ &= (\alpha \cdot 0 + \alpha) \cup (\alpha \cdot 1 + \alpha)\\ &= \alpha \cup \{\alpha + \alpha\}\\ &= \alpha + \alpha, \quad \text{since } \alpha \subseteq \alpha + \alpha \text{ by VI.10.2.}\end{aligned}$$

$(iv)$: Fix $\alpha < \beta$. We do induction on $\gamma$: Let $\gamma = 0$. Then $\alpha \cdot 0 = \beta \cdot 0$. Done. Next, consider $\gamma = \lambda + 1$. Then

$$\begin{aligned}\alpha \cdot (\lambda + 1) &= \alpha \cdot \lambda + \alpha\\ &= \leq \beta \cdot \lambda + \alpha \quad \text{by I.H. and VI.10.11}(ii)\\ &< \beta \,.\, \lambda + \beta \quad \text{by VI.10.2}\\ &= \beta \cdot (\lambda + 1)\end{aligned}$$

Finally, let Lim$(\gamma)$, and assume (I.H.) that $\alpha \cdot \lambda \leq \beta \cdot \lambda$ for all $\lambda < \gamma$. Thus, $\alpha \cdot \gamma = \bigcup_{\lambda<\gamma} \alpha \cdot \lambda \subseteq \bigcup_{\lambda<\gamma} \beta \cdot \lambda = \beta \cdot \gamma$.

$(v)$: The $\leftarrow$ is by VI.10.14. The $\rightarrow$ is by VI.10.14 and trichotomy.

$(vi)$: The result holds for $\alpha = 0$ (by $(i)$), so let $\alpha > 0$ and do induction on $\gamma$. The case $\gamma = 0$ is $\alpha \cdot (\beta + 0) = \alpha \cdot \beta = \alpha \cdot \beta + 0 = \alpha \cdot \beta + \alpha \cdot 0$, using $(i)$ for the last "=". Let $\gamma = \lambda + 1$, and assume the obvious I.H. Then

$$\begin{aligned}\alpha \cdot \big(\beta + (\lambda + 1)\big) &= \alpha \cdot \big((\beta + \lambda) + 1\big)\\ &= \alpha \cdot (\beta + \lambda) + \alpha\\ &= (\alpha \cdot \beta + \alpha \cdot \lambda) + \alpha \quad \text{by I.H.}\\ &= \alpha \cdot \beta + (\alpha \cdot \lambda + \alpha)\\ &= \alpha \cdot \beta + \alpha \cdot (\lambda + 1)\end{aligned}$$

Finally, let Lim$(\gamma)$, and assume the claim (I.H.) for all $\lambda < \gamma$. Now,

$$\begin{aligned}\alpha \cdot (\beta + \gamma) &= \alpha \cdot (\beta + \sup\{\lambda : \lambda < \gamma\})\\ &= \alpha \cdot (\sup\{\beta + \lambda : \lambda < \gamma\}) \quad \text{by continuity of } + \text{ (VI.5.36, VI.10.2)}\\ &= \sup\{\alpha \cdot (\beta + \lambda) : \lambda < \gamma\} \quad \text{by continuity of } \cdot \text{ (VI.5.36, VI.10.14)}\\ &\qquad\qquad \text{(recall that we are in the case } \alpha > 0)\\ &= \sup\{\alpha \cdot \beta + \alpha \cdot \lambda : \lambda < \gamma\} \quad \text{by I.H.}\\ &= \alpha \cdot \beta + \sup\{\alpha \cdot \lambda : \lambda < \gamma\} \quad \text{by continuity of } +\\ &= \alpha \cdot \beta + \alpha \cdot \gamma \quad \text{by VI.10.13}\end{aligned}$$

$(vii)$: We do induction on $\gamma$ (assume throughout that $\alpha \neq 0 \neq \beta$, since otherwise the result reads $0 = 0$). When $\gamma = 0$, we get $\alpha \cdot (\beta \cdot 0) = \alpha \cdot 0 = 0$. Also, $(\alpha \cdot \beta) \cdot 0 = 0$. Done.

Let $\gamma = \lambda + 1$. Then $\alpha \cdot (\beta \cdot (\lambda + 1)) = \alpha \cdot (\beta \cdot \lambda + \beta) = \alpha \cdot (\beta \cdot \lambda) + \alpha \cdot \beta = (\alpha \cdot \beta) \cdot \lambda + \alpha \cdot \beta = (\alpha \cdot \beta) \cdot (\lambda + 1)$, where the second "=" uses distributivity, and the third one the obvious I.H.

Let now $\mathrm{Lim}(\gamma)$. Then, arguing as in $(vi)$, using continuity of $\cdot$,

$$\begin{aligned}\alpha \cdot (\beta \cdot \gamma) &= \alpha \cdot (\beta \cdot \sup\{\lambda : \lambda < \gamma\})\\ &= \alpha \cdot \sup\{\beta \cdot \lambda : \lambda < \gamma\}\\ &= \sup\{\alpha \cdot (\beta \cdot \lambda) : \lambda < \gamma\}\\ &= \sup\{(\alpha \cdot \beta) \cdot \lambda : \lambda < \gamma\} \quad \text{by I.H.}\\ &= (\alpha \cdot \beta) \cdot \gamma \quad \text{by VI.10.13.}\end{aligned}$$

$(viii)$: By Exercise VI.33,

$$\alpha + \beta = \bigcup\{\alpha + (\gamma + 1) : \gamma < \beta\} \tag{4}$$

under the assumptions. On the other hand,

$$\alpha \cdot \beta = \bigcup\{\alpha \cdot (\gamma + 1) : \gamma < \beta\} \tag{5}$$

We thus take as I.H. that $1 < \alpha$ and $1 < \gamma$ yield $\alpha + \gamma \le \alpha \cdot \gamma$. Therefore, (4) and (5) yield the result for $\beta > 1$, by the I.H. and the strict monotonicity of $\lambda\gamma.\alpha + (\gamma + 1)$ and $\lambda\gamma.\alpha \cdot (\gamma + 1)$.

$(ix)$: $\alpha \cdot \beta = \bigcup_{\gamma \in \beta}(\alpha \cdot \gamma + \alpha) \supseteq \alpha$ by VI.10.11$(ii)$ and the fact that the union is nonempty. We have proved more under the assumptions: $0 < \alpha \le \alpha \cdot \beta$. □

**VI.10.20 Remark.** Multiplication of ordinals is not commutative. For example, $\omega \cdot 2 = \omega + \omega > \omega$. On the other hand, $2 \cdot \omega = \bigcup\{2 \cdot n : n \in \omega\}$, since $\mathrm{Lim}(\omega)$. Now $\{2 \cdot n : n \in \omega\} \subseteq \omega$; hence

$$\bigcup\{2 \cdot n : n \in \omega\} \subseteq \omega$$

The $\subseteq$ above graduates to $=$, since the fact that $\mathrm{Lim}(2 \cdot \omega)$ precludes $\subset$. Thus, $\omega \cdot 2 > 2 \cdot \omega$.

There are two more conclusions to be drawn from this example:

(1) The "right" distributive law does *not* hold. For example, $(1 + 1) \cdot \omega = 2 \cdot \omega = \omega < \omega + \omega = \omega \cdot 2$.
(2) VI.10.19$(iv)$ cannot be sharpened. Indeed, $1 < 2$, yet $1 \cdot \omega = 2 \cdot \omega$. □

**VI.10.21 Proposition (Division with Remainder).** *Given $\alpha$ and $\beta > 0$, there are* unique *ordinals $\pi$ and $\upsilon$ such that*

(1) *$\alpha = \beta \cdot \pi + \upsilon$,*
(2) *$\pi \le \alpha$ and $\upsilon < \beta$.*

$\pi$ is the *quotient* and $\upsilon$ is the *remainder* of the division of $\alpha$ by $\beta$.

This extends the well-known theorem of Euclid from $\omega$ to all of On.

*Proof. Existence*. If $\alpha = 0$, then take $\pi = \upsilon = 0$. So let $\alpha > 0$. Since $\beta \cdot 0 = 0 < \alpha$, the set $X = \{\theta : \beta \cdot \theta \leq \alpha\}$ is not empty (why *set*?). If $\theta > \alpha$, then

$$\begin{aligned} \beta \cdot \theta &\geq 1 \cdot \theta && \text{by VI.10.19} \\ &= \theta && \text{by VI.10.19} \\ &> \alpha \end{aligned}$$

Hence $\theta \notin X$. Contrapositively, $\theta \in X \to \theta \leq \alpha$. Thus $\sup X \leq \alpha$. We claim that

$$\pi = \sup X \tag{1}$$

works. So far ($\pi \leq \alpha$), so good. We want to propose a partnering $\upsilon$.

Now, using VI.5.36 and VI.10.19,

$$\begin{aligned} \beta \cdot \pi &= \beta \cdot \sup X \\ &= \sup\{\beta \cdot \theta : \theta \in X\} \\ &\leq \alpha \end{aligned} \tag{2}$$

By VI.10.11($v$) and (2), there is an $\upsilon$ such that

$$\alpha = \beta \cdot \pi + \upsilon \tag{3}$$

with

$$\upsilon = 0 \quad \text{iff} \quad \text{(2) is equality} \tag{4}$$

We next show that $\upsilon < \beta$. If not,

*Case* $\beta = \upsilon$. Then (3) yields (by VI.10.13) that $\alpha = \beta \cdot (\pi + 1)$; hence $\pi + 1 \in X$, contradicting (1).

*Case* $\beta < \upsilon$. Then (VI.10.11($v$)) there is a $\gamma > 0$ such that $\upsilon = \beta + \gamma$, and (3) yields

$$\begin{aligned} \alpha &= \beta \cdot \pi + (\beta + \gamma) \\ &= \beta \cdot (\pi + 1) + \gamma \end{aligned}$$

again yielding $\pi + 1 \in X$ by VI.10.11($v$), thus contradicting (1). We have settled existence.

*Uniqueness*. Let

$$\alpha = \beta \cdot \pi + \upsilon = \beta \cdot \pi' + \upsilon' \tag{5}$$

where $\upsilon < \beta$ and $\upsilon' < \beta$.

Let $\pi < \pi'$. Then $\pi' = \pi + \gamma$ for some $\gamma > 0$; hence

$$\alpha = \beta \cdot (\pi + \gamma) + \upsilon' = \beta \cdot \pi + (\beta \cdot \gamma + \upsilon')$$

Now

$$\begin{aligned} \upsilon &< \beta \\ &= \beta \cdot 1 \\ &\leq \beta \cdot \gamma \\ &\leq \beta \cdot \gamma + \upsilon' \end{aligned}$$

Hence $\beta \cdot \pi + \upsilon < \beta \cdot \pi + (\beta \cdot \gamma + \upsilon') = \beta \cdot \pi' + \upsilon'$, contradicting (5).

Similarly, $\pi > \pi'$ is untenable; hence $\pi = \pi'$. Thus $\upsilon = \upsilon'$ by VI.10.11$(iii)$. □

**VI.10.22 Corollary.** *For* $\alpha > 0$*,* $\text{Lim}(\alpha)$ *iff* $(\exists\beta)\omega \cdot \beta = \alpha$ *iff* $2 \cdot \alpha = \alpha$*.*

*Proof.* Let $\text{Lim}(\alpha)$, and divide $\alpha$ by $\omega$ to get (by VI.10.21)

$$\alpha = \omega \cdot \pi + \upsilon$$

Now, $\upsilon < \omega$; hence it is a natural number. If $\upsilon > 0$, then $\upsilon = n + 1$ $(n \in \omega)$; hence $\alpha = \omega \cdot \pi + (n + 1) = (\omega \cdot \pi + n) + 1$, a successor. This contradicts the assumption, so $\upsilon = 0$.

Next, say $0 < \alpha = \omega \cdot \beta$. Then $2 \cdot \alpha = 2 \cdot (\omega \cdot \beta) = (2 \cdot \omega) \cdot \beta = \omega \cdot \beta = \alpha$, where we have used VI.10.20 in the penultimate "=".

Finally, let $0 < \alpha = 2 \cdot \alpha$, and suppose that $\alpha = \beta + 1$ for some $\beta$. Then

$$\begin{aligned} \alpha &= 2 \cdot (\beta + 1) \\ &= 2 \cdot \beta + 2 \\ &\geq 1 \cdot \beta + 2 \quad \text{by VI.10.19} \\ &= \beta + 2 \\ &> \beta + 1 = \alpha \end{aligned}$$

a contradiction. So $\text{Lim}(\alpha)$. □

We conclude this section with the operation of exponentiation on ordinals, once again using the corresponding operation on the natural numbers for motivation. Therefore we will iterate multiplication.

**VI.10.23 Definition (Exponentiation of Ordinals).** The unique function $P(\alpha, \beta)$ defined by the recursion below will be denoted by $\alpha^{\cdot\beta}$:

$$\begin{aligned} P(\alpha, 0) &= 1 \\ P(\alpha, \beta + 1) &= P(\alpha, \beta) \cdot \alpha \\ \text{for } \operatorname{Lim}(\beta), \quad P(\alpha, \beta) &= \sup\{P(\alpha, \gamma) : \gamma < \beta\} \end{aligned} \qquad \square$$

The "$\cdot$" in $\alpha^{\cdot\beta}$ is an annoying convention used to distinguish ordinal exponentiation from cardinal exponentiation, the latter being (usually) privileged not to need the "$\cdot$".

So far we have kept the notation for ordinal operations "natural", by using the same symbolism as that used on the natural numbers. As justification we invoke priority: In our development we first developed the natural numbers, and we denoted $n \cup \{n\}$ by $n + 1$ (as most people justifiably do), which induced (or forced) our subsequent notation, $+$ and $\cdot$, first on the natural numbers and then on ordinals. We decided that we did not want to ask the reader to write $m \dotplus n$ from some point onwards, when he means to add $m$ and $n$. Note, however, that some authors use $\dotplus$ and $\bullet$ respectively, although they may start off with the notation $n + 1$ for $n \cup \{n\}$.

It is clear that the above recursion also defines exponentiation over $\omega$, provided the case $\operatorname{Lim}(\alpha)$ is dropped, as it is irrelevant over $\omega$.

**VI.10.24 Remark.** If $\alpha > 0$, then $\alpha^{\cdot\beta} > 0$. Indeed, $\alpha^{\cdot 0} = 1 > 0$. Furthermore, assuming that $\alpha^{\cdot\beta} > 0$ (I.H.), we get that

$$\alpha^{\cdot\beta+1} = \alpha^{\cdot\beta} \cdot \alpha > 0$$

by VI.10.19($ix$). Finally, if $\operatorname{Lim}(\beta)$ and $\alpha^{\cdot\gamma} > 0$ for all $\gamma < \beta$ (I.H.), then

$$\alpha^{\cdot\beta} = \sup\{\alpha^{\cdot\gamma} : \gamma < \beta\} > 0 \qquad \square$$

**VI.10.25 Proposition.** *If $\alpha > 0$, then $\lambda\beta.\alpha^{\cdot\beta}$ is weakly normal. If $\alpha > 1$, then it is normal.*

*Proof.* Since $\alpha^{\cdot\beta} > 0$ by VI.10.24, we have $\alpha^{\cdot\beta+1} = \alpha^{\cdot\beta} \cdot \alpha \geq \alpha^{\cdot\beta}$ by VI.10.19, with "$>$" if $\alpha > 1$. The result follows from VI.5.38 and VI.5.39. □

**VI.10.26 Corollary.** *If $\alpha > 1$ and $\operatorname{Lim}(\beta)$, then $\operatorname{Lim}(\alpha^{\cdot\beta})$.*

**VI.10.27 Proposition (Some Properties of Ordinal Exponentiation).**

$(i)$ $0^{\cdot\alpha} = 0$ *iff* $\alpha$ *is a successor; otherwise* $0^{\cdot\alpha} = 1$
$(ii)$ $1^{\cdot\alpha} = 1$
$(iii)$ $\alpha > 1 \to (\alpha^{\cdot\beta} < \alpha^{\cdot\gamma} \leftrightarrow \beta < \gamma)$
$(iv)$ $\alpha > 0 \to \alpha^{\cdot\beta+\gamma} = \alpha^{\cdot\beta} \cdot \alpha^{\cdot\gamma}$
$(v)$ $\alpha > 0 \to (\alpha^{\cdot\beta})^{\cdot\gamma} = \alpha^{\cdot\beta\cdot\gamma}$
$(vi)$ $\alpha > 1 \wedge \beta > 0 \to 1 < \alpha^{\cdot\beta}$
$(vii)$ $\alpha > 1 \wedge \beta > 1 \to \alpha \cdot \beta \leq \alpha^{\cdot\beta}$.

*Proof.* $(i)$: $0^{\cdot\beta+1} = 0^{\cdot\beta} \cdot 0 = 0$ by VI.10.19. By VI.10.23, $0^{\cdot 0} = 1$. Now if $\mathrm{Lim}(\beta)$, then $0^{\cdot\beta} = \sup\{0^{\cdot\gamma} : \gamma < \beta\} \geq 1$, since $0 < \beta$. Assume next (I.H.) that whenever $\gamma < \beta$ and $\mathrm{Lim}(\gamma)$, then $0^{\cdot\gamma} = 1$. It follows that $0^{\cdot\beta} = \sup\{0^{\cdot\gamma} : \gamma < \beta\} \leq 1$.

For $(ii)$, $1^{\cdot 0} = 1$, and $1^{\cdot\alpha+1} = 1^{\cdot\alpha} \cdot 1 = 1 \cdot 1 = 1$ using the obvious I.H. Finally, let $\mathrm{Lim}(\alpha)$ and $1^{\cdot\beta} = 1$ for all $\beta < \alpha$ (I.H.). Then $1^{\cdot\alpha} = \sup\{1^{\cdot\beta} : \beta < \alpha\} = \sup\{1\} = 1$.

$(iii)$: By VI.10.25 and trichotomy.

$(iv)$: We do induction on $\gamma$. First, $\alpha^{\cdot\beta+0} = \alpha^{\cdot\beta} = \alpha^{\cdot\beta} \cdot 1 = \alpha^{\cdot\beta} \cdot \alpha^{\cdot 0}$. This settles the basis. Next,

$$\begin{aligned}
\alpha^{\cdot\beta+(\gamma+1)} &= \alpha^{\cdot(\beta+\gamma)+1} \\
&= \alpha^{\cdot\beta+\gamma} \cdot \alpha \quad \text{by VI.10.23} \\
&= (\alpha^{\cdot\beta} \cdot \alpha^{\cdot\gamma}) \cdot \alpha \quad \text{by the obvious I.H.} \\
&= \alpha^{\cdot\beta} \cdot (\alpha^{\cdot\gamma} \cdot \alpha) \\
&= \alpha^{\cdot\beta} \cdot \alpha^{\cdot\gamma+1} \quad \text{by VI.10.23}
\end{aligned}$$

Finally, let $\mathrm{Lim}(\gamma)$, and assume the claim for all $\delta < \gamma$. By VI.5.35 and VI.10.25, $\lambda\beta.\alpha^{\cdot\beta}$ is *continuous*. Therefore,

$$\begin{aligned}
\alpha^{\cdot\beta+\gamma} &= \alpha^{\cdot\beta+\sup\{\delta\,:\,\delta<\gamma\}} \\
&= \alpha^{\cdot\sup\{\beta+\delta\,:\,\delta<\gamma\}} \\
&= \sup\{\alpha^{\cdot\beta+\delta} : \delta < \gamma\} \\
&= \sup\{\alpha^{\cdot\beta} \cdot \alpha^{\cdot\delta} : \delta < \gamma\} \quad \text{by the I.H.} \\
&= \alpha^{\cdot\beta} \cdot \sup\{\alpha^{\cdot\delta} : \delta < \gamma\} \quad \text{by continuity of } \cdot \text{ and by } \alpha^{\cdot\beta} > 0 \\
&= \alpha^{\cdot\beta} \cdot \alpha^{\cdot\gamma}
\end{aligned}$$

$(v)$: A similar routine calculation proves this case.

$(vi)$: $1 = \alpha^{\cdot 0}$. Now use $(iii)$.

$(vii)$: Going for a contradiction, let $\beta > 1$ be *smallest* for which $(vii)$ fails, i.e.,

$$\alpha^{\cdot\beta} < \alpha \cdot \beta \tag{1}$$

Is it the case that Lim$(\beta)$? If so, $\alpha \cdot \beta = \sup\{\alpha \cdot \delta : \delta < \beta\}$ and Lim$(\alpha \cdot \beta)$ (cf. VI.10.15); thus, by (1), there is a $\delta < \beta$ such that

$$\alpha^{\cdot\beta} < \alpha \cdot \delta \tag{2}$$

By (2),

$$\delta > 1$$

since otherwise $\alpha^{\cdot\beta} < \alpha = \alpha^{\cdot 1}$, contradicting $(iii)$ (recall, $\alpha > 1,\ \beta > 1$). Now, by $(iii)$,

$$\begin{aligned} \alpha^{\cdot\delta} &< \alpha^{\cdot\beta} \\ &< \alpha \cdot \delta, \quad \text{by (2)} \end{aligned}$$

This contradicts the minimality of $\beta$, so we must have $\beta = \gamma + 1$ for some $\gamma$. Clearly, $\gamma > 1$; otherwise $\gamma = 1$ (why?) and (1) says that

$$\alpha \cdot \alpha = \alpha^{\cdot 2} < \alpha \cdot 2 = \alpha + \alpha$$

which cannot be, by VI.10.19$(viii)$. By minimality of $\beta$,

$$\alpha \cdot \gamma \leq \alpha^{\cdot\gamma}$$

Hence

$$(\alpha \cdot \gamma) \cdot \alpha \leq \alpha^{\cdot\gamma} \cdot \alpha = \alpha^{\cdot\beta} \tag{3}$$

Since $\beta = \gamma + 1 < \gamma + \alpha \leq \gamma \cdot \alpha$ by VI.10.19$(viii)$, (3) yields

$$\alpha \cdot \beta < \alpha \cdot (\gamma \cdot \alpha) = (\alpha \cdot \gamma) \cdot \alpha \leq \alpha^{\cdot\beta}$$

contradicting (1). □

**VI.10.28 Example.** $(\alpha \cdot \beta)^{\cdot\gamma} \neq \alpha^{\cdot\gamma} \cdot \beta^{\cdot\gamma}$ in general. For example,

$$(2 \cdot 2)^{\cdot\omega} = (2^{\cdot 2})^{\cdot\omega} = 2^{\cdot 2 \cdot \omega} = 2^{\cdot\omega} \tag{1}$$

while

$$2^{\cdot\omega} \cdot 2^{\cdot\omega} = 2^{\cdot\omega+\omega} \tag{2}$$

We see that the right hand sides of (1) and (2) are different by VI.10.27$(iii)$; therefore so are the left hand sides. □

**VI.10.29 Remark.** Since $\lambda\alpha.\omega^{\cdot\alpha}$ is normal, it has arbitrarily large fixed points. Such fixed points were called "$\varepsilon$-numbers" by Cantor.

In particular, the reader can readily verify that $\sup\{\omega, \omega^{\cdot\omega}, \omega^{\cdot\omega^{\cdot\omega}}, \ldots\}$ is an $\varepsilon$-number, the smallest one above $\omega$. □

Additional material on the arithmetic of ordinals can be found in the Exercises section and in the references Bachmann (1955), Kamke (1950), Levy (1979), Monk (1969), Sierpiński (1965), Tarski (1956).

## VI.11. Exercises

**VI.1.** If $\mathbb{P}$ has MC and $\mathbb{Q} \subseteq \mathbb{P}$, then $\mathbb{Q}$ has MC.

**VI.2.** If $\mathbb{P}$ is left-narrow, then $\mathbb{P}^n\langle a\rangle$ is a set for all $n > 0$ in $\omega$ and all $a$.

**VI.3.** Prove that if an order $<$ is left-narrow, then it has MC iff every nonempty set has a $<$-minimal element.

(*Hint.* Only the if part is non-trivial. Start with $a \in \mathbb{A}$. If $a$ is minimal, fine. Else show that any minimal element in the set $<\langle a\rangle \cap \mathbb{A}$ is minimal in $\mathbb{A}$.)

**VI.4.** Prove that if a relation $\mathbb{P}$ is left-narrow, then it has MC iff every nonempty *set* has a $\mathbb{P}$-minimal element.

(*Hint.* Work with $\mathbb{P}^+$.)

**VI.5.** Prove the claims in the ☡–☡ passage in Remark VI.2.26.

**VI.6.** Prove that if $A \subseteq B$ and $A$ is a transitive set, then $C(B, x) = x$ for all $x \in A$, where $C$ is Mostowski's collapsing function (VI.2.38).
(*Hint.* Use $\in$-induction.)

**VI.7.** With reference to VI.4.3, prove that $\big[(\{1\}, <)\big]_{\cong}$ is a proper class, where "$<$" is the standard order on $\omega$.

**VI.8.** Prove that the relation $<$ defined on On in VI.4.9 is transitive.

**VI.9.** Prove Theorem VI.4.30 directly by explicitly using the recursion (1) of VI.4.32.

**VI.10.** Prove VI.3.23 for WO sets by using the comparability of ordinals and Theorem VI.4.30 (proved via VI.4.32).

**VI.11.** For $\alpha > 0$ prove that $\mathrm{Lim}(\alpha)$ iff for all $\beta < \alpha$ there is a $\gamma$ such that $\beta < \gamma < \alpha$.

**VI.12.** For each $\alpha \neq 0$ show that $\sup^+ \alpha = \alpha$.

**VI.13.** Prove that $\mathrm{Lim}(\alpha)$ iff $\alpha \neq 0$ and $\alpha = \bigcup \alpha$.

**VI.14.** Prove that if a set $\emptyset \neq A \subseteq \mathrm{On}$ does not have a maximum, then $\sup(A)$ is a limit ordinal.

**VI.15.** Prove that there are arbitrarily large limit ordinals, that is, for each $\alpha$ there is a $\beta > \alpha$ such that $\mathrm{Lim}(\beta)$. This problem addresses questions raised (and answers promised) following V.1.2.

(*Hint.* By induction over $\omega$ define the sequence $f(0) = \alpha$ and $f(n+1) = f(n) + 1$. Argue that (1): if $\beta = \sup \mathrm{ran}(f)$, then $\mathrm{Lim}(\beta)$; and (2): $\alpha < \beta$.)

**VI.16.** Prove that if $f$ is a weakly continuous On-sequence, of ordinals that moreover satisfies $(\forall\alpha) f(\alpha) \leq f(\alpha + 1)$, then $f$ is non-decreasing and hence is weakly normal.

**VI.17.** Prove that the composition of normal functions is normal.

**VI.18.** Prove that if $f$ is a normal transfinite On-sequence, then, for any $\gamma$, it has a fixed point $\beta$ such that $\gamma < \beta$. Check that your proof (along the lines of that for the Knaster-Tarski theorem) furnishes the smallest fixed point greater than $\gamma$.

**VI.19.** Prove the Knaster-Tarski fixpoint theorem (VI.5.47) under the weakened assumption that in the PO set $(A, <)$ every chain has a least upper bound.

**VI.20.** Refer to the proof of VI.5.47. For the $\gamma$ chosen, prove that $s_{<\gamma} = s_\gamma$.

**VI.21.** Prove that for all $\alpha$, $sp(V_N(\alpha)) \subseteq N$.

**VI.22.** Show that, for all $\alpha$, $\beta$, $V_N(\alpha) \in V_N(\beta)$ implies $\alpha < \beta$.

**VI.23.** Show that $\rho(V_N(\alpha)) = \alpha + 1$.

**VI.24.** Define "standard rank" by $rk_N(x) = \min\{\alpha : x \subseteq N \cup V_N(\alpha)\}$. Show that $rk_N(\alpha) = \alpha$.

**VI.25.** Relate $\rho_N$ and $rk_N$. Show that for all sets $x$, $\rho_N(x) = rk_N(x) + 1$.

**VI.26.** Complete the proof of VI.7.2.

**VI.27.** Substantiate the comment made following VI.7.5.

**VI.28.** Show for the $J$ of Section VI.7 that $J(\alpha, \beta) = \{J(\sigma, \tau) : \langle\sigma, \tau\rangle \lhd \langle\alpha, \beta\rangle\}$.

**VI.29.** Show for the $\lhd$ of Section VI.7 that $\alpha^2 = \lhd(\langle 0, \alpha\rangle)$ for all $\alpha$.

**VI.30.** Prove that the function $\lambda\alpha.J[\alpha \times \alpha]$ is increasing (order-preserving).

**VI.31.** Prove that the function $\lambda\alpha.J[\alpha \times \alpha]$ has arbitrarily large fixed points.

(*Hint.* Prove that it is normal.)

**VI.32.** Prove that ordinal addition is absolute for transitive models of ZF.

**VI.33.** Prove that if $\beta > 0$, then $\alpha + \beta = \sup^+\{\alpha + \gamma : \gamma < \beta\}$.

**VI.34.** Prove that $1 + \alpha = \alpha$ iff $\omega \leq \alpha$.

**VI.35.** Let $(X_\beta, <_\beta) \cong (Y_\beta, <_\beta)$ for all $\beta < \alpha$. Show that

$$\operatorname*{cat}_{\beta<\alpha}(X_\beta, <_\alpha) \cong \operatorname*{cat}_{\beta<\alpha}(Y_\beta, <_\alpha)$$

**VI.36.** Let $(X, <_1)$ and $(Y, <_2)$ be disjoint WO sets. Define $<$ on $X \cup Y$ by

$$\begin{array}{lll} a < b & \text{iff} & \{a, b\} \subseteq X \wedge a <_1 b \vee \\ & & \{a, b\} \subseteq Y \wedge a <_2 b \vee \\ & & a \in X \wedge b \in Y \end{array}$$

Show that $(X \dot{+} Y, <_*) \cong (X \cup Y, <)$.

**VI.37.** (*Left cancellation in ordinal addition.*) Show that if $\alpha + \beta = \alpha + \gamma$, then $\beta = \gamma$.

**VI.38.** (*Right cancellation in ordinal addition does not hold.*) Show by an example that $\beta + \alpha = \gamma + \alpha \not\rightarrow \beta = \gamma$.

**VI.39.** Prove that ordinal multiplication is absolute for transitive models of ZF.

**VI.40.** Show that $\alpha > 0$ implies $\beta \leq \alpha \cdot \beta$.

**VI.41.** Show that if $\alpha > 0$ and $\beta > 1$, then $\alpha < \alpha \cdot \beta$.

**VI.42.** (*Left cancellation in ordinal multiplication.*) Show that if $\alpha > 0$ and $\alpha \cdot \beta = \alpha \cdot \gamma$, then $\beta = \gamma$.

**VI.43.** (*Right cancellation in ordinal multiplication does not hold.*) Show by an example that $\alpha > 0 \wedge \beta \cdot \alpha = \gamma \cdot \alpha \not\rightarrow \beta = \gamma$.

**VI.44.** For any $0 < n \in \omega$, show that $n \cdot \omega = \omega$.

**VI.45.** Show that $\alpha > 0$ is a limit iff for every $0 < n < \omega$, $\alpha = n \cdot \alpha$.

**VI.46.** Prove that ordinal exponentiation is absolute for transitive models of ZF.

**VI.47.** Show that $\alpha^{\cdot 1} = \alpha$ and $\alpha^{\cdot 2} = \alpha \cdot \alpha$.

**VI.48.** Prove VI.10.27($v$).

**VI.49.** Prove that for all $m, n$ in $\omega$, $m^{\cdot n} \in \omega$.

**VI.50.** Prove that for all $m, n, k$ in $\omega$, $(m \cdot n)^{\cdot k} = m^{\cdot k} \cdot n^{\cdot k}$.

**VI.51.** Show for all $\alpha > 1$ that $\alpha^{\cdot \beta} \geq \beta$. Can $\geq$ be sharpened to $>$? Why?

**VI.52.** Prove that $\operatorname{Lim}(\alpha)$ implies that $(\alpha + n)^{\cdot \omega} = \alpha^{\cdot \omega}$ for all $n \in \omega$.

**VI.53.** Prove that if the formula $\mathscr{A}$ has no quantifiers, then it is absolute for any class $\mathbb{M}$.

In the following few exercises models of fragments of ZFC are being sought. We mean $(U, \in)$-models.

**VI.54.** Show that $V(\omega)$ is a model for ZFC$-$infinity (i.e., satisfies all the ZFC axioms except that for infinity). Indeed, infinity fails here. By the way, this shows that infinity is not implied by the remaining axioms.

**VI.55.** Show that $V(\alpha)$ is a model for ZFC$-$collection, for any limit ordinal $\alpha > \omega$.

**VI.56.** Find a limit ordinal $\alpha > \omega$ such that the collection axiom is false in $V(\alpha)$. By the way, this shows that collection is not implied by the remaining axioms.

(*Hint.* Experiment with $\alpha = \omega + \omega$.)

**VI.57.** Prove that the structure $(\mathrm{On}, U, \in)$ is not a model of ZFC.

**VI.58.** Let $N$ be a set of urelements such that $f : N \to n$ is a 1-1 correspondence for some $n \in \omega$. Prove that $V_N(\omega)$ is a model of ZFC$-$infinity. (It fails infinity).

**VI.59.** Let $N$ be a set of urelements such that $f : N \to \omega$ is a 1-1 correspondence. Prove that $V_N(\omega)$ is a model of ZFC$-\{$infinity, collection$\}$. (It fails both infinity and collection.)

**VI.60.** Show that for any transitive class $\mathbb{M}$, $\mathbf{P}^{\mathbb{M}}(A) = \mathbb{M} \cap \mathbf{P}(A)$.

**VI.61.** Complete the proof of Lemma VI.8.16.

**VI.62.** Prove that $\mathbb{L}_N$ satisfies *global choice*. That is, show that there is a function $\mathbb{F}$ on $\mathbb{L}_N$ such that for any set $\emptyset \neq x \in \mathbb{L}_N$, $\mathbb{F}(x) \in x$.

# VII

# Cardinality

In Chapter VI, among other things, we studied the WO sets and learnt how to measure their *length* with the help of ordinal numbers. A consequence of the axiom of choice was (Theorem VI.5.50) that *every set* can be well-ordered and therefore every set can be assigned a length.[†]

In the present chapter we turn to another aspect of set size, namely its number of elements, or *cardinality*. It will turn out that for *finite* sets length and cardinality are measured by the same (finite) ordinal; thus, in particular, finite sets have a unique length. As was already remarked, the situation with *infinite* sets is much less clean intuitively, and several WO sets of differing lengths can have the same number of elements (e.g., $\omega$, $\omega + 1$, $\omega + 2$, etc).

The following section will formalize the notions of "finite" and "infinite" sets. Intuitively, a set is finite if the process of removing its elements, one at a time, will terminate; it is infinite otherwise.[‡]

Thus for finite sets the process implicitly assigns the numbers $1, 2, 3, \ldots$ to the first, second, third, … removed items. Since the process terminates, there will be a natural number assigned to the last removed item. Evidently this number equals the *cardinality*, or number of elements, of the set.

[†] This length is not unique in general. For example, the set $\omega \cup \{\omega\}$ can be assigned both the lengths $\omega + 1$ and $\omega$.

[‡] This intuitive idea is for motivation only, and it will not be used anywhere except in the informal discussion here. One can easily get into trouble if "time" is taken too literally. For example, let us deplete $\omega$ in finite time! Start by removing 0. Exactly 1 hour later remove 1; exactly $1/2$ hour later remove $2; \ldots$ ; exactly $1/2^n$ hour later remove $n + 1$; and so on, in the obvious pattern. It takes just $1 + 1/2 + 1/2^2 + \cdots + 1/2^n + \cdots = 2$ hours to complete the task. Yet, $\omega$ is intuitively infinite. Of course, we would not have had this informal "paradox" if we were careful to say explicitly that we spend exactly the same amount of time between any two consecutive removals of elements.

In the infinite case it is not clear *a priori* how to assign a "number" that denotes the cardinality of the set. Thus the issue is temporarily postponed, and one first worries about whether or not two infinite sets have the *same* number of elements. This is an easier problem to address, and it *can* be addressed before we settle the question of what "number of elements" means. Indeed, any two sets (infinite or not) clearly have the same number of elements if we can match each element of one with a unique element of the other in such a way that no unmatched elements are left on either side. Technically, two sets have the same cardinality iff there is a 1-1 correspondence between them. Let us now formalize this discussion and see where it leads.

## VII.1. Finite vs. Infinite

**VII.1.1 Definition.** Two sets $A$ and $B$ are said to be *equinumerous* or *equipotent*, in symbols $A \sim B$, iff there is a 1-1 correspondence $f : A \to B$.

The negation of $\sim$ is denoted by $\not\sim$. □

**VII.1.2 Exercise (Informal).** Show that $\sim$ is an equivalence relation on the universe (of sets) $\mathbb{U}_M$.
(*Hint.* For *reflexivity* note that the function $\emptyset : \emptyset \to \emptyset$ proves the special case $\emptyset \sim \emptyset$.) □

**VII.1.3 Definition.** A set $A$ is *finite* iff $A \sim n$, where $n \in \omega$. We call $n$ *the cardinality* or *cardinal number* of $A$, and write $|A| = n$ in this case.

A set which is not finite is *infinite*. □

☡ **VII.1.4 Remark.** According to the above definition and the hint in Exercise VII.1.2, $\emptyset$ is finite. Furthermore, each $n \in \omega$ is finite, and $|n| = n$.

Corollary VII.1.8 below shows that *the* cardinality of a finite set is indeed unique, for it is impossible to have $n \sim A \sim m$ and $n \neq m$ with $m$ and $n$ in $\omega$. □ ☡

**VII.1.5 Example.** Let $\mathbb{E}$ denote the set of even numbers. Then $\mathbb{E} \sim \omega$.

Indeed, the function $f : \omega \to \mathbb{E}$ given by $f = \lambda n.2n$ is a 1-1 correspondence. □

We now embark on showing that the definition of finite set is "reasonable", that is, it leads to the (intuitively) expected properties of finite sets.

**VII.1.6 Proposition.** *If $x \subset n \in \omega$, then there is no* onto *function $f : x \to n$.*

$x$ is not necessarily a natural number, so that “$\subset$” here is more general than “$<$”.

*Proof.* Induction on $n$ in $\omega - \{0\}$.

*Basis*: $n = 1$: Then the only function $f : x \to n$ is $\emptyset : \emptyset \to 1$, which is clearly not onto.

*I.H.*: Assume that if $n = k$, then there is no onto function $f : x \to n$ for *any* $x \subset n$.

We show, by contradiction, that the situation is unchanged when $n = k + 1$. Let instead $f : x \to k + 1$ be onto, where $x \neq \emptyset$.[†] So let $H = f^{-1}\langle k\rangle$. By ontoness, $\emptyset \neq H$, and, of course, $H \subseteq x$.

*Case 1.* $k \notin x$. Then $g = f \restriction (x - H)$ is onto $k$, and $x - H \subset k$, contradicting the I.H.

*Case 2.* $k \in x$. If $f(k)\uparrow$, then use $x - \{k\}$ and go back to Case 1. Otherwise, let $k \neq m = f(k)$ and set $g = \big(f - \{\langle k, m\rangle\} \cup (H \times \{k\})\big) \cup (H \times \{m\})$. Then $g : x - \{k\} \to k$ is onto, which contradicts the I.H. Finally, if $k = f(k)$, then $f - (H \times \{k\}) : x - H \to k$ is onto, and we have contradicted the I.H. once more. □

**VII.1.7 Corollary.** *If $x \subset n \in \omega$, then $x \not\sim n$.*

**VII.1.8 Corollary.** *If $m < n \in \omega$, then $m \not\sim n$.*

One refers to Corollary VII.1.8 as the *pigeon-hole principle*, in that if you have $n$ pigeons and $m$ holes (or vice versa) then there is no way to put exactly one pigeon in each hole so that no pigeon is left out (and no hole is empty).

**VII.1.9 Proposition.** *If $x \subset n \in \omega$, then $x$ is finite and $|x| < n$.*

$x$ is not necessarily a natural number, so that “$\subset$” here is more general than “$<$”.

*Proof.* $x$ is well-ordered by $\in$ (or $<$) as a subset of $n$. Thus, for some $\alpha$,

$$(x, \in) \cong (\alpha, \in)$$

In particular, $\alpha \sim x$, say, via the 1-1 correspondence $f : \alpha \to x$.

By VII.1.7, $\alpha \neq n$. Suppose that $n < \alpha$. Let $y = \operatorname{ran}(f \restriction n)$. Then $n \sim y$ via $f \restriction n$, and $y \subseteq x \subset n$, contradicting VII.1.7. Thus, $\alpha < n$. That is, $\alpha$ is a natural number $m$, $x \sim m$, and $m < n$. □

[†] The case $x = \emptyset$ cannot lead to onto functions, as seen in the basis step; therefore it is not considered here.

**VII.1.10 Corollary.** *If $A$ is finite and $B \subseteq A$, then $B$ is finite and $|B| \leq |A|$.*

*Proof.* Let $f : A \to n$ be a 1-1 correspondence for some $n \in \omega$. Then $B \sim \operatorname{ran}(f \restriction B) \subseteq n$.

By Proposition VII.1.9, $\operatorname{ran}(f \restriction B) \sim m$ for some $m \leq n$; thus $B \sim m$ (by transitivity of $\sim$). □

**VII.1.11 Corollary.** *$A$ is finite iff there is an onto $f : n \to A$ for some $n \in \omega$.*

*Proof. If part.* Let $f : n \to A$ be onto. Define $g$ on $A$ by $g(x) = \min f^{-1}\langle x \rangle$. Then $g : A \to \operatorname{ran}(g) \subseteq n$ is a 1-1 correspondence; hence $|A| = |\operatorname{ran}(g)| \leq n$.

*Only-if part.* Let $f : n \to A$ be a 1-1 correspondence. Then $f$ is onto. □

It is clear from the proof of the if part that $f$ need not be total.

**VII.1.12 Corollary.** *If $A$ and $B$ are finite, then $A \sim B$ iff $|A| = |B|$.*

*Proof. If part.* Let $|A| = |B| = n \in \omega$. Let $h : n \to A$ and $g : n \to B$ be 1-1 correspondences. Then $g \circ h^{-1} : A \to B$ is a 1-1 correspondence.

*Only-if part.* Let $f : A \to B$, $h : A \to n$ and $g : B \to m$ be 1-1 correspondences, where $m < n$. The diagram below establishes $m \sim n$, a contradiction:

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "h"'] & B \arrow[d, "g"] \\
n \arrow[r, "g \circ f \circ h^{-1}"'] & m
\end{tikzcd}$$

□

**VII.1.13 Proposition.** *For all $n \in \omega$ there is no $f$ such that $f : n \to \omega$ is* onto.

*Proof.* Induction on $n$.

*Basis*: $n = 0$: The result is immediate.

*I.H.*: Assume the assertion for $n \leq k$. Proceeding by contradiction, assume that $f : k + 1 \to \omega$ is onto and let $H = f^{-1}\langle 0 \rangle$. Hence $k + 1 \supseteq H \neq \emptyset$ by ontoness. Thus, $k + 1 - H \sim m < k + 1$ for some $m$, by VII.1.9. Let $g : m \to k + 1 - H$ be a 1-1 correspondence. The diagram below shows that $h \circ g : m \to \omega$ is onto, contradicting I.H., since $m \leq k$:

$$\begin{tikzcd}
m \arrow[r, "g"] & K + 1 - H \arrow[r, "h = \lambda x.\left(f \restriction (k+1-H)\right)(x) - 1"] & \omega
\end{tikzcd}$$

□

**VII.1.14 Corollary.** *$\omega$ is infinite.*

Before we turn our attention to infinite sets, we will look into finite sets more carefully, at the same time establishing a few facts about *inductively defined sets* and a technique of proving properties of finite sets by some sort of induction.

**VII.1.15 Definition.** Given a class $\mathbb{S}$ and an $n$-ary function $f$ for some $n \in \omega$, we say that $\mathbb{S}$ is *closed under $f$*, or is *$f$-closed*, iff $\operatorname{ran}(f \restriction \mathbb{S}^n) \subseteq \mathbb{S}$.

If $f$ is a set, then it is called an *$n$-ary operation,* or *rule, on* $\mathbb{S}$. If $\mathscr{F}$ is a set of rules and $\mathbb{S}$ is a class, then "$\mathbb{S}$ is *$\mathscr{F}$-closed*" means that $\mathbb{S}$ is closed under *all* $f \in \mathscr{F}$. □

The reader is familiar with operations on sets. For example, $+$ is a total 2-ary operation on the real numbers, $\mathbb{R}$. We prefer to call 2-ary operations *binary*. Also, $\lambda x.1/x$ is a nontotal 1-ary operation on $\mathbb{R}$. We call 1-ary operations *unary*.

We also note that $\emptyset$ is closed under any $f$ and that if for a choice of an $n$-ary $f$ and class $\mathbb{S}$ it is the case that $\operatorname{ran}(f \restriction \mathbb{S}^n) = \emptyset$, then $\mathbb{S}$ is $f$-closed.

The requirement that "operations" (or "rules") be *sets* does not limit the range of applicability of the concept, while it simplifies the technicalities. For example, it is meaningful to have a *set* of rules, since, so restricted, they are objects which can be collected into a class or set. Further justification for this restriction is embedded in the proof of Proposition VII.1.19 below. The material below formalizes work presented informally in Section I.2 to bootstrap our theory.

**VII.1.16 Definition.** Given a set $\mathscr{I}$ and a set of operations on $\mathscr{F}$. We say that a set $S$ is *inductively,* or *recursively*, defined by $\mathscr{I}$ (the *initial objects*) and $\mathscr{F}$ (the set of *operations* or *rules*) iff $S$ is the *$\subseteq$-smallest* set that satisfies both of the following conditions:

(a) $\mathscr{I} \subseteq S$.
(b) $S$ is $\mathscr{F}$-closed.

Under these conditions, we also say that $S$ is *the closure* of $\mathscr{I}$ under $\mathscr{F}$, in symbols $S = \mathrm{Cl}(\mathscr{I}, \mathscr{F})$. □

**VII.1.17 Remark.** We clarify "$\subseteq$-smallest": If after replacing $S$ by the set $T$ in (a) and (b) we find that $T$ satisfies (a) and (b), then $S \subseteq T$. □

**VII.1.18 Example.** $\omega$ is inductively defined by $\mathscr{I} = \{0\}$ and $\mathscr{F} = \big\{\lambda x.x \cup \{x\}\big\}$, where we may take as $\operatorname{dom}(\lambda x.x \cup \{x\})$ $\omega$ itself, or any ordinal $\alpha$ such that $\omega < \alpha$.

Indeed, first, $\omega$ satisfies (a) and (b) of Definition VII.1.16. Secondly, let a set $T$ also satisfy (a) and (b) with respect to the given $\mathscr{I}$ and $\mathscr{F}$.

That is, $0 \in T$ and $(\forall x)(x \in T \rightarrow x \cup \{x\} \in T)$. By induction over $\omega$, $\omega \subseteq T$; $\omega$ is $\subseteq$-smallest. □

**VII.1.19 Proposition.** *Given the sets $\mathscr{I}$ and $\mathscr{F}$ of Definition VII.1.16, a unique set* $\mathrm{Cl}(\mathscr{I}, \mathscr{F})$ *exists and is equal to $\bigcap_{x \in \mathbb{J}} x$, where $\mathbb{J}$ is the class of all sets $x$ satisfying* (a) *and* (b).

*Proof.* First, let $X = \mathscr{I} \cup \bigcup_{f \in \mathscr{F}} \mathrm{ran}(f)$. By Exercise VII.3, $X$ is a set that satisfies (a) and (b). Thus $X \in \mathbb{J}$, and hence $S = \bigcap_{x \in \mathbb{J}} x$ is a set, being a subclass of $X$.

Next, it is easy to verify that $S$ satisfies (a) and (b). (See Exercise VII.3.) Finally, $S$ is $\subseteq$-smallest, for if a set $Q$ satisfies (a) and (b), then $Q \in \mathbb{J}$.

The above establishes *existence*. For *uniqueness* use the $\subseteq$-smallest property. (See Exercise VII.3.) □

We next note that there are two reasons justifying the term "inductively defined", or "recursively defined", for sets such as $S = \mathrm{Cl}(\mathscr{I}, \mathscr{F})$.

First, the set $S$ is defined in terms of ("smaller", or "earlier", instances of) itself (starting with $\mathscr{I}$). For, (b) of Definition VII.1.16 says that if we know $S$ up to a certain "extent", or "stage", then we can enlarge $S$ by applying to its current version the operations in $\mathscr{F}$.

Second, the definition allows us to prove properties of all elements of $S$ by *induction with respect to the formation,* or *definition*, of $S$. We also say, by induction *over* $S$.

Such inductive definitions appear frequently in logic and mathematics, as we have already witnessed, which was the reason that compelled us to present an informal version of these results early on.

**VII.1.20 Theorem (Induction over an Inductively Defined Set).** *Let $\mathscr{P}(x)$ be a formula. Then $\big(\forall x \in \mathrm{Cl}(\mathscr{I}, \mathscr{F})\big)\mathscr{P}(x)$ is derivable from the assumptions*

(i) $(\forall x \in \mathscr{I})\mathscr{P}(x)$ *(basis), and*
(ii) for each *$n$-ary $f \in \mathscr{F}$,*

$$(\forall \vec{a}_n)\big(f(\vec{a}_n) \downarrow\rightarrow \mathscr{P}(a_1) \wedge \cdots \wedge \mathscr{P}(a_n) \rightarrow \mathscr{P}(f(\vec{a}_n))\big)$$

Condition (ii) in the theorem is also pronounced "$\mathscr{P}(x)$ *propagates* with each operation in $\mathscr{F}$". The part "$\mathscr{P}(a_1) \wedge \cdots \wedge \mathscr{P}(a_n)$" is the I.H. for $f$.

*Proof.* Let $\mathbb{P}$ be the class $\{x : \mathscr{P}(x)\}$. By (i) $\mathscr{I} \subseteq \mathbb{P}$, and by (ii) $\mathbb{P}$ is $\mathscr{F}$-closed. The set $X = \mathscr{I} \cup \bigcup_{f \in \mathscr{F}} \operatorname{ran}(f)$ is also $\mathscr{F}$-closed, and $\mathscr{I} \subseteq X$.

Thus $Z = X \cap \mathbb{P}$ is a set which satisfies (a) and (b) of Definition VII.1.16. Hence $\mathrm{Cl}(\mathscr{I}, \mathscr{F}) \subseteq Z$ by Proposition VII.1.19, from which follows $\mathrm{Cl}(\mathscr{I}, \mathscr{F}) \subseteq \mathbb{P}$. □

As the above proof suggests, proving by induction with respect to $\mathrm{Cl}(\mathscr{I}, \mathscr{F})$ – or $(\mathscr{I}, \mathscr{F})$-induction – that $\big(\forall x \in \mathrm{Cl}(\mathscr{I}, \mathscr{F})\big)\mathscr{P}$ amounts to proving that the class $\mathbb{P} = \{x : \mathscr{P}(x)\}$ is $\mathscr{F}$-closed and that, moreover, $\mathscr{I} \subseteq \mathbb{P}$.

**VII.1.21 Definition.** Given $\mathscr{I}$ and $\mathscr{F}$. An $n$-tuple $\langle x_1, \ldots, x_n \rangle$ is a $(\mathscr{I}, \mathscr{F})$-*derivation*, or simply *derivation* if $\mathscr{I}$ and $\mathscr{F}$ are understood, iff for each $i = 1, \ldots, n$, at least one of the following holds:

(a) $x_i \in \mathscr{I}$, or
(b) $x_i = f(x_{j_1}, \ldots, x_{j_k})$, where $j_m < i$ for $m = 1, \ldots, k$ and $f \in \mathscr{F}$ is a $k$-ary operation.[†]

We say that $x_n$ is $(\mathscr{I}, \mathscr{F})$-*derived*, or just *derived* if $\mathscr{I}$ and $\mathscr{F}$ are understood, by the derivation $\langle x_1, \ldots, x_n \rangle$. □

**VII.1.22 Remark.** It is clear that if $\langle x_1, \ldots, x_n \rangle$ is a derivation, then so is each $\langle x_1, \ldots, x_k \rangle$ for $0 < k < n$. □

**VII.1.23 Example.** Let $\mathscr{I} = \{0\}$, $\mathscr{F} = \big\{\lambda x.x \cup \{x\}\big\}$. Then $\langle 0, 1, 2 \rangle$ and $\langle 0, 1, 0, 0, 1, 1, 0, 2 \rangle$ are $(\mathscr{I}, \mathscr{F})$-derivations. They both derive 2. □

**VII.1.24 Theorem.** *For any $\mathscr{I}$ and $\mathscr{F}$, $\{x : x$ is $(\mathscr{I}, \mathscr{F})$-derived$\} = \mathrm{Cl}\,(\mathscr{I}, \mathscr{F})$.*

*Proof.* Let us denote by $\mathbb{D}$ the class $\{x : x \text{ is } (\mathscr{I}, \mathscr{F})\text{-derived}\}$. First, we do $(\mathscr{I}, \mathscr{F})$-induction to show $\mathrm{Cl}\,(\mathscr{I}, \mathscr{F}) \subseteq \mathbb{D}$.

*Basis*: $\mathscr{I} \subseteq \mathbb{D}$, since for each $a \in \mathscr{I}$, $\langle a \rangle$ is a derivation of $a$.

We next show that $\mathbb{D}$ is $\mathscr{F}$-closed. So let $f \in \mathscr{F}$ be $n$-ary and let $f(\vec{a}_n) \downarrow$, where $a_i \in \mathbb{D}$ for $i = 1, \ldots, n$. By definition of $\mathbb{D}$, there are derivations $\langle \ldots, a_1 \rangle, \ldots, \langle \ldots, a_n \rangle$.

Then $\langle \ldots, a_1, \ldots, \ldots, a_n \rangle$ is a derivation (see Exercise VII.4), and therefore so is $\langle \ldots, a_1, \ldots, \ldots, a_n, f(\vec{a}_n) \rangle$ (why?). It follows that $f(\vec{a}_n) \in \mathbb{D}$. Thus $\mathbb{D}$ is $f$-closed, and hence $\mathscr{F}$-closed, since $f \in \mathscr{F}$ was arbitrary.

By induction over $\mathrm{Cl}\,(\mathscr{I}, \mathscr{F})$, we have obtained $\mathrm{Cl}\,(\mathscr{I}, \mathscr{F}) \subseteq \mathbb{D}$.

[†] We also say that $x_i$ is obtained from $k$ *previous* objects in the derivation by the application of a $k$-ary operation from $\mathscr{F}$.

Next, to show the opposite inclusion, we do induction in $\omega - \{0\}$ with respect to the length, $n$, of $(\mathscr{I}, \mathscr{F})$-derivations.

*Basis*: $n = 1$: Let $a \in \mathbb{D}$, where $\langle a \rangle$ is a derivation. Then $a \in \mathscr{I} \subseteq \mathrm{Cl}(\mathscr{I}, \mathscr{F})$.

*I.H.*: Assume the claim for $n \leq k$. Let $n = k+1$, and $\langle a_1, \ldots, a_k, a \rangle$ be a derivation of $a \in \mathbb{D}$. If $a \in \mathscr{I}$, then $a \in \mathrm{Cl}(\mathscr{I}, \mathscr{F})$ as in the basis step. Let then $a = f(a_{j_1}, \ldots, a_{j_r})$. By the I.H., $\{a_{j_1}, \ldots, a_{j_r}\} \subseteq \mathrm{Cl}(\mathscr{I}, \mathscr{F})$, since each of $\langle \ldots, a_{j_1} \rangle, \ldots, \langle \ldots, a_{j_r} \rangle$ is a derivation of length $\leq k$. But $\mathrm{Cl}(\mathscr{I}, \mathscr{F})$ is closed under $f$. □

In particular, $\mathbb{D}$ is a set.

The above theorem provides an alternative characterization of the set $\mathrm{Cl}(\mathscr{I}, \mathscr{F})$, which is more convenient when we want to prove that such and such an $x$ is in the set. On the other hand, the original definition (VII.1.16) is more flexible to use when we try to prove properties of *all* the elements of $\mathrm{Cl}(\mathscr{I}, \mathscr{F})$, in which case we use $(\mathscr{I}, \mathscr{F})$-induction. In such inductive proofs we do not need to refer to the natural numbers, not even implicitly, since we do not employ derivations.

Before we proceed with an alternative definition of finite sets, due to Whitehead and Russell, we present one more result on inductive definitions, which properly belongs here and will also be used later (for example, in the proof of the Cantor-Bernstein theorem).

**VII.1.25 Definition.** Let $X$ be a set. An *operator over* $X$ is a function $\Gamma : \mathbf{P}(X) \to \mathbf{P}(X)$. $\Gamma$ is *monotone* iff for every $S \subseteq T \subseteq X$, $\Gamma(S) \subseteq \Gamma(T)$. Thus, a monotone operator is total.

A set $S \subseteq X$ is $\Gamma$-*closed* iff $\Gamma(S) \subseteq S$. □

**VII.1.26 Example.** Let $\mathscr{I}$ be a set, and $\mathscr{F}$ a set of operations. For each $f \in \mathscr{F}$ we denote its arity by $n(f)$. $X$ will denote $\mathscr{I} \cup \bigcup_{f \in \mathscr{F}} \mathrm{ran}(f)$.

Define $\Gamma_{\mathscr{I},\mathscr{F}}$, for simplicity referred to as just $\Gamma$ in the balance of the example, by $\Gamma(Z) = \mathscr{I} \cup \bigcup_{f \in \mathscr{F}} \mathrm{ran}(f \restriction Z^{n(f)})$, for all $Z \subseteq X$.

Thus a set of initial objects, $\mathscr{I}$, and a set of operations, $\mathscr{F}$, give rise to an operator over $X$. It is clear that $\Gamma$ is monotone, since $S \subseteq T \subseteq X$ implies $\mathrm{ran}(f \restriction S^{n(f)}) \subseteq \mathrm{ran}(f \restriction T^{n(f)})$. □

**VII.1.27 Theorem.** *If* $\Gamma$ *is a monotone operator over the set* $X$*, then the set*

$$S = \bigcap_{\substack{Z \subseteq X \\ \Gamma(Z) \subseteq Z}} Z$$

*satisfies* $\Gamma(S) = S$.

We call $S$ a *fixed point* or *fixpoint* of $\Gamma$. It turns out that $S$ is the $\subseteq$-*smallest* fixed point of $\Gamma$.

*Proof.* Let $J = \{Z : Z \subseteq X \wedge \Gamma(Z) \subseteq Z\}$. Now $J$ is a nonempty set, since $X \in J \subseteq \mathbf{P}(X)$. Hence, $S$ is a set.

Next, we establish that $\Gamma(S) \subseteq S$, i.e., that $\Gamma(\bigcap_{Z\in J} Z) \subseteq S$. Indeed,

$$\begin{aligned}\Gamma\Big(\bigcap_{Z\in J} Z\Big) &\subseteq \bigcap_{Z\in J} \Gamma(Z) \qquad \Big[\text{by monotonicity } \Gamma\Big(\bigcap_{Z\in J} Z\Big) \subseteq \Gamma(Z)\Big] \\ &\subseteq \bigcap_{Z\in J} Z = S\end{aligned}$$

To conclude, we need to show that $S \subseteq \Gamma(S)$. We proceed by contradiction: Let, instead, $x \in S - \Gamma(S)$. By monotonicity of $\Gamma$, $\Gamma(S - \{x\}) \subseteq \Gamma(S) \subseteq S$, and, since $x \notin \Gamma(S)$, we have $x \notin \Gamma(S - \{x\})$ as well. Thus $\Gamma(S - \{x\}) \subseteq S - \{x\}$; hence $S - \{x\} \in J$, and therefore $S = \bigcap_{Z\in J} Z \subseteq S - \{x\}$, a contradiction. □

**VII.1.28 Remark.** $\Gamma(S) \subseteq S$ implies that $S \in J$, and therefore $S$ is the $\subseteq$-smallest set in $J$. If now $\Gamma(T) = T$, then also $\Gamma(T) \subseteq T$; hence $T \in J$ and consequently $S \subseteq T$. Thus the claim of the preceding note, that $S$ is the $\subseteq$-smallest fixed point of $\Gamma$, is correct.

One usually denotes this $\subseteq$-smallest fixed point of $\Gamma$ by $\overline{\Gamma}$ or $\Gamma^{\infty}$. □

**VII.1.29 Corollary ($\boldsymbol{\Gamma}$-Induction, or Induction over $\boldsymbol{\overline{\Gamma}}$).** $(\forall x \in \overline{\Gamma})\mathscr{T}(x)$, *where* $\Gamma$ *is an operator over a set* $X$, *is derivable from a proof that* $\{x \in X : \mathscr{T}(x)\}$ *is* $\Gamma$-*closed.*

*Proof.* Let $Z = \{x \in X : \mathscr{T}(x)\}$. By assumption, $\Gamma(Z) \subseteq Z$. Thus $Z \in J$ (where $J$ is as in VII.1.27); hence $\overline{\Gamma} \subseteq Z$ and therefore $(\forall x \in \overline{\Gamma})\mathscr{T}(x)$. □

**VII.1.30 Remark.** For an abstraction of what we are doing here see VI.5.47 and VI.5.49. Here the PO set $(A, <)$ is $(\mathbf{P}(X), \subset)$, and $f$ is $\Gamma$.

Monotone operators are also called *inductive*. VII.1.29 provides a justification for the name "inductive", for it says that $\overline{\Gamma}$ has the "property" $\mathscr{T}(x)$ if it happens that the property "propagates with" $\Gamma$: If $Z$ is the set of all $x \in X$ which satisfy $\mathscr{T}(x)$, then all the elements of $\Gamma(Z)$ also satisfy the property. □

**VII.1.31 Example.** We conclude Example VII.1.26 by showing that the $\subseteq$-smallest fixed points of inductive operators generalize the notion of inductively defined sets.[†]

[†] This generalization is *proper*, i.e., there are fixed points $\overline{\Gamma}$ which cannot be inductively defined as in Definition VII.1.16. These $\overline{\Gamma}$ require infinitary operations, i.e., operations with infinitely many arguments.

Let $S = \mathrm{Cl}(\mathscr{I}, \mathscr{F})$ and $X$ be as in Example VII.1.26. We will show that $S = \overline{\Gamma}_{\mathscr{I},\mathscr{F}}$. First,

$$\Gamma_{\mathscr{I},\mathscr{F}}(Z) \subseteq Z \leftrightarrow \mathscr{I} \cup \bigcup_{f \in \mathscr{F}} \mathrm{ran}(f \restriction Z^{n(f)}) \subseteq Z$$

by definition of $\Gamma_{\mathscr{I},\mathscr{F}}$ (Example VII.1.26). In words,

$$\Gamma_{\mathscr{I},\mathscr{F}}(Z) \subseteq Z \quad \text{iff} \quad \mathscr{I} \subseteq Z \text{ and } Z \text{ is } \mathscr{F}\text{-closed.} \tag{1}$$

By Theorem VII.1.27,

$$\begin{aligned} \overline{\Gamma}_{\mathscr{I},\mathscr{F}} &= \bigcap_{\substack{Z \subseteq X \\ \Gamma_{\mathscr{I},\mathscr{F}}(Z) \subseteq Z}} Z \\ &= \bigcap_{\substack{\mathscr{I} \subseteq Z \subseteq X \\ Z \text{ is } \mathscr{F}\text{-closed.}}} Z \qquad \text{by (1)} \\ &= S \end{aligned}$$

Finally, let us recognize $(\mathscr{I}, \mathscr{F})$-induction as $\Gamma_{\mathscr{I},\mathscr{F}}$-induction.

To prove $(\forall x \in S)\mathscr{P}(x)$ by $(\mathscr{I}, \mathscr{F})$-induction, we let $\mathbb{P}$ be the class $\{x : \mathscr{P}(x)\}$ and prove that $\mathscr{I} \subseteq \mathbb{P}$ and $\mathbb{P}$ is $\mathscr{F}$-closed. If this plan succeeds, then we have actually proved (see the proof of Theorem VII.1.20) that the *set* $Z = X \cap \mathbb{P} = \{x \in X : \mathscr{P}(x)\}$ satisfies $\mathscr{I} \subseteq Z$ and is $\mathscr{F}$-closed. By (1), this is tantamount to proving that $Z$ is $\Gamma_{\mathscr{I},\mathscr{F}}$-closed. By Corollary VII.1.29, this proves $(\forall x \in \overline{\Gamma}_{\mathscr{I},\mathscr{F}})\mathscr{P}(x)$, i.e., $(\forall x \in S)\mathscr{P}(x)$, by $\Gamma_{\mathscr{I},\mathscr{F}}$-induction. □

We will return to inductive operators in Section VII.7. To conclude the present section, we resume the study of finite sets.

Definition VII.1.3 was based on the intuitive notion of depleting a finite set in "finite time" by successively removing its elements, one at a time. The following alternative definition due to Whitehead and Russell (1912) (see also Levy (1979)) *builds*, rather than depletes, a finite set from "scratch" (i.e., from ∅) in "finite time", by successively *adding* elements to it.

The definition given below is a variant of the original one, chosen in the context of the preceding groundwork on inductive definitions – and especially *derivations* – so as to make it clear that we are on the right track towards characterizing "finite" (see the following remark).

We will use the term WR-finite[†] until we can show that the notions of "finite" and "WR-finite" are equivalent.

[†] **W**hitehead-**R**ussell-finite.

**VII.1.32 Definition.** A set $A$ is *WR-finite* iff $A \in \mathrm{Cl}(\mathscr{I}, \mathscr{F})$, where $\mathscr{I} = \{\emptyset\}$ and $\mathscr{F} = \big\{f_y : \mathrm{dom}(f_y) = \mathbf{P}(A) \wedge y \in A \wedge f_y = \lambda x.x \cup \{y\}\big\}$.

If $A$ is not WR-finite, then it is *WR-infinite*. □

**VII.1.33 Remark.** Since $A$ is a set, so is $\mathscr{F}$. By Theorem VII.1.24, $A$ is WR-finite iff there is some derivation $\langle\emptyset, \ldots, A\rangle$ of $A$ such that at each *non-redundant* step[†] a set $x \cup \{y\}$ occurs, where $x$ is available at an earlier step of the derivation and $y \in A$.

Thus in a "finite number of steps" we obtain $A$ by collecting its elements together, one at a time, starting from $\emptyset$. So the definition is reasonable. Note that the notion of natural number was only used *implicitly* (via the derivation concept) in this remark; it does *not* occur in the Definition VII.1.32, not even implicitly. □

**VII.1.34 Proposition.** *$\emptyset$ is WR-finite.*

*Proof.* Let $\mathscr{I} = \{\emptyset\}$ and $\mathscr{F} = \emptyset$. Since $\mathscr{I} \subseteq \mathrm{Cl}(\mathscr{I}, \mathscr{F})$, it follows that $\emptyset \in \mathrm{Cl}(\mathscr{I}, \mathscr{F})$. □

**VII.1.35 Proposition.** *If $A$ is WR-finite, then so is $A \cup \{y\}$ for any $y$.*

*Proof.* We look at the interesting case where $y \notin A$. By assumption, $A \in \mathrm{Cl}(\mathscr{I}, \mathscr{F})$, where $\mathscr{I} = \{\emptyset\}$, and $\mathscr{F}$ is the set of all the total functions $\lambda x.x \cup \{z\}$ on $\mathbf{P}(A)$, for all $z \in A$.

Let $\mathscr{G} = \mathscr{F}' \cup \big\{\lambda x.x \cup \{y\}\big\}$, where $\mathscr{F}'$ contains exactly the $\mathscr{F}$-functions extended to $\mathbf{P}(A \cup \{y\})$, so that for all $z \in A \cup \{y\}$, $\mathrm{dom}(\lambda x.x \cup \{z\}) = \mathbf{P}(A \cup \{y\})$. A trivial $(\mathscr{I}, \mathscr{F})$-induction shows that $\mathrm{Cl}(\mathscr{I}, \mathscr{F}) \subseteq \mathrm{Cl}(\mathscr{I}, \mathscr{G})$ (see Exercise VII.6). Hence, $A \in \mathrm{Cl}(\mathscr{I}, \mathscr{G})$ and therefore $A \cup \{y\} \in \mathrm{Cl}(\mathscr{I}, \mathscr{G})$, since $\mathrm{Cl}(\mathscr{I}, \mathscr{G})$ is closed under $\lambda x.x \cup \{y\}$. □

**VII.1.36 Remark.** Here is an easier alternative proof: Let $\langle\emptyset, \ldots, A\rangle$ be a $(\mathscr{I}, \mathscr{F})$-derivation. Then $\langle\emptyset, \ldots, A, A \cup \{y\}\rangle$ is a $(\mathscr{I}, \mathscr{G})$-derivation; hence $A \cup \{y\} \in \mathrm{Cl}(\mathscr{I}, \mathscr{G})$.

We prefer the original proof, because it avoids any reliance on the natural numbers. □

[†] At any step of the derivation we may place $\emptyset$; such a step is *redundant* in that it does not help to progress with the formation of $A$.

**VII.1.37 Theorem (Induction on WR-Finite Sets) (Zermelo (1909)).** *Let $\mathscr{P}(x)$ be a formula. To prove*

$$(\forall x)\big(x \text{ is WR-finite} \to \mathscr{P}(x)\big)$$

*it suffices to prove the following two things:*

(a) $\mathscr{P}(\emptyset)$*, and*

(b)

$$(\forall x)(\forall y)\big(x \text{ is WR-finite} \to \mathscr{P}(x) \to \mathscr{P}(x \cup \{y\})\big)$$

*Proof.* Let $\mathscr{P}(x)$ be as above, and $A$ be WR-finite. Then $A \in \mathrm{Cl}(\mathscr{I}, \mathscr{F})$, where $\mathscr{I} = \{\emptyset\}$ and $\mathscr{F}$ is as in Definition VII.1.32. Let $S = \{x : x \text{ is WR-finite} \wedge x \subseteq A \wedge \mathscr{P}(x)\}$.

By (a) and VII.1.34, $\mathscr{I} \subseteq S$.

By (b) and Proposition VII.1.35, $S$ is $\mathscr{F}$-closed. Therefore, by $(\mathscr{I}, \mathscr{F})$-induction, $\mathrm{Cl}(\mathscr{I}, \mathscr{F}) \subseteq S$; hence $A \in S$. In particular, $\mathscr{P}(A)$. □

**VII.1.38 Theorem.** *$A$ is finite iff it is WR-finite.*

*Proof. If part.* We show that for some $n \in \omega$, $A \sim n$. The proof is by induction on WR-finite sets.

*Basis*: $\emptyset \sim 0$.

*I.H.*: Let $x$ be WR-finite, and for some $n \in \omega$, $f : x \to n$ be a 1-1 correspondence. Consider $x \cup \{y\}$, and show this set to be equinumerous with some natural number. If $y \in x$, then the result is the I.H. itself.

So let $y \notin x$. Then $f \cup \{\langle y, n\rangle\}$ provides a 1-1 correspondence $x \cup \{y\} \to n \cup \{n\} = n + 1$.

*Only-if part.* Let $f : n \to A$ be a 1-1 correspondence. Then $f[n] = A$. By Exercises VII.7 and VII.8, $A$ is WR-finite. □

From now on we drop the qualification "WR-" from "finite". What we are left with from all this, besides a better understanding of finite sets, is the useful proof technique of induction on finite sets.

**VII.1.39 Theorem.** *Let $|A| = n$, and $<$ be a well-ordering on $A$. Then $(A, <) \cong n$.*[†]

[†] By "$\cong n$" we mean, of course, "$\cong (n, \in)$". We are following the convention of Section VI.4 in writing "$\cong \alpha$" as a short form of "$\cong (\alpha, \in)$" for ordinals.

*Proof.* By induction on $n$.

*Basis*: $n = 0$. The result is trivial.

*I.H.*: Assume the claim for $n = k$. Let $n = k + 1$. By Exercise VII.10, $A$ has a $<$-maximal element, say $a$. Now, $a$ is also $<$-maximum, since $<$ is a total order. That is, $x < a$ for all $x \in A - \{a\}$.

Now, $|A - \{a\}| = k$ (see Exercise VII.12) and the I.H. yield $(A - \{a\}, <) \cong k$. By pairing $a$ with $k$, we extend the previous $\cong$ to $(A, <) \cong k + 1$. □

The above result establishes the claim made in the preamble to this chapter, namely, that there is a *unique* "length" for each finite set and that this length coincides with the set's cardinality. We add that, of course, every finite set is well-orderable, a well-ordering being induced by $A \sim |A|$ (see VI.3.12).

## VII.2. Enumerable Sets

**VII.2.1 Definition.** A set $S$ is *enumerable* iff $S \sim \omega$. If $S$ is either finite or enumerable, then it is called *countable*.

If a set is not countable, then it is called *uncountable*. □

Some authors use the term *denumerable* for enumerable. Also, the term *at most enumerable* is sometimes used for countable.

**VII.2.2 Example.** According to Definition VII.2.1 each finite set is also countable. We also observe that $\omega$ is enumerable (since $\omega \sim \omega$), so enumerable sets exist. Do *uncountable* sets exist? In other words, are there infinite sets which are not enumerable? Cantor, as we will see in the next section, answered this affirmatively. □

**VII.2.3 Example.** The set of the even natural numbers, $\mathbb{E}$, is enumerable, since $\lambda x.2x : \omega \to \mathbb{E}$ is a 1-1 correspondence. A similar comment is true for the set of the odd natural numbers. □

**VII.2.4 Example.** Every enumerable set is infinite. Indeed, if $A \sim \omega$, then (see Exercise VII.2) $A$ is finite iff $\omega$ is. But $\omega$ is not finite.

If now $A \subseteq B$ and $A$ is enumerable, then $B$ is infinite. This is so because of Corollary VII.1.10. □

**VII.2.5 Theorem.** *If $A \subseteq \omega$, then $A$ is countable.*

*Proof.* If $A$ is finite, then we are done. So let $A$ be infinite.
Define $f$ by induction on $n$ as follows:

$$f(0) = \min A$$

and if $n > 0$, $\qquad (i)$

$$f(n) \simeq \min\big(A - \operatorname{ran}(f \restriction n)\big)$$

Observe that

(1) Since the recursion $(i)$ is pure, $\operatorname{dom}(f) \leq \omega$. Say, $\operatorname{dom}(f) = n \in \omega$ (for some $n$). Thus, $A = f[n]$.[†] By Exercise VII.18 (or VII.7), $A$ is finite, a contradiction. Thus $f$ is total on $\omega$.

(2) $f$ is 1-1. Indeed, let $n \neq m$, where we assume, without loss of generality, that $m < n$. Hence $f(m) \in \operatorname{ran}(f \restriction n)$; therefore $f(n) \neq f(m)$ by the second part of $(i)$.[‡]

(3) $A = \operatorname{ran}(f)$. Let us assume instead that, for some $m$, $m \in A - \operatorname{ran}(f)$. Since $\omega \sim \operatorname{ran}(f)$ (why?), $\operatorname{ran}(f)$ is infinite; therefore, for some $n$,

$$m \leq f(n) \qquad (ii)$$

for, otherwise, $(\forall n \in \omega) f(n) < m$, i.e., $\operatorname{ran}(f) \subseteq m$, making $\operatorname{ran}(f)$ finite. Indeed, $(ii)$ graduates to $m < f(n)$, the strict inequality being justified from $m \notin \operatorname{ran}(f)$. This last observation is inconsistent with the definition of $f(n)$ (second equation of $(i)$) since both $m$ and $f(n)$ are in $A - \operatorname{ran}(f \restriction n)$.

Items (1) through (3) establish that $\omega \sim A$. □

**VII.2.6 Corollary.** *A nonempty set $A$ is countable iff there is an onto function $f : \omega \to A$.*[§]

*Proof. Only-if part.* Let $A$ be finite and $f : n \to A$ be a 1-1 correspondence for some $n \in \omega$. Trivially, $f$ is a (nontotal) function on $\omega$, and is onto $A$.

If, on the other hand, $A$ is infinite, then there is a 1-1 correspondence $f : \omega \to A$ for some $f$. This $f$ is onto.

*If part.* If $A$ is finite, we are done. So let $A$ be infinite, and let $f : \omega \to A$ be onto.

[†] $f(n) \uparrow$ entails $A \subseteq \operatorname{ran}(f \restriction n)$.

[‡] See also Exercise VII.20.

[§] We emphasize that $f$ need *not* be total.

By V.3.9, there is a right inverse, $g : A \to \omega$, of $f$, in the sense that $f \circ g = \mathbf{1}$, where $\mathbf{1}$ is the identity on $A$.

By V.3.4, $g$ is total and 1-1; thus $A \sim \mathrm{ran}(g)$. By Exercise VII.2, $\mathrm{ran}(g)$ is infinite; by Theorem VII.2.5, $\omega \sim \mathrm{ran}(g)$; hence $\omega \sim A$. (See also Exercise VII.21.) □

It is clear that, if we want, we can state the corollary so that $f$ is total. Indeed, if $f : A \to B$ is nontotal but onto, then we can always extend it to a total *and* onto function $h$ by taking $h = f \cup \{\langle x, b\rangle : x \in A - \mathrm{dom}(f)\}$, where $b$ is any fixed element of $B$. Thus, whereas the original definition (Definition VII.2.1) of $A$ being enumerable requires that an enumeration *without repetitions* exists (this is the 1-1 correspondence $f : \omega \to A$), we now have relaxed this by saying, via Corollary VII.2.6, that a nonempty set $A$ is countable iff an enumeration exists (possibly *with* repetitions – the 1-1-ness requirement being dropped).

**VII.2.7 Example.** If $A$ is countable and $B \subseteq A$, then $B$ is countable. Indeed, if $B = \emptyset$, then the result is immediate.

So, let $B \neq \emptyset$, and let (by Corollary VII.2.6) $f : \omega \to A$ be onto. The total function $i = \lambda x.x$ on $B$ is 1-1. Thus the inverse relation, $i^{-1}$, is an onto (but nontotal, unless $A = B$) function $i^{-1} : A \to B$. Clearly $i^{-1} \circ f : \omega \to B$ is onto. □

**VII.2.8 Example.** If $A$ and $B$ are countable, then so are $A \cap B$ and $A - B$. This follows from $A \cap B \subseteq A$ and $A - B \subseteq A$.

Note that the hypothesis could be weakened to simply require that just $A$ be countable. □

**VII.2.9 Proposition.** *$\omega \sim \omega \times \omega$.*

*Proof.* By VI.7.8. □

There is a more "elementary" proof that avoids the $J$ of VI.7.4 and uses just multiplication and addition on $\omega$.

We start with the total function $f = \lambda mn.(m+n)\cdot(m+n)+m$ on $\omega^2$. (By the way, $\omega^2$ is in the Cartesian product sense throughout. Ordinal exponentiation would have used an exponent "$\cdot 2$" instead, and cardinal exponentiation we have not introduced yet.)

One can easily derive that $f$ is 1-1, relying on what we know about ordinal addition and multiplication (cf. VI.10.11 and VI.10.19). Indeed, assume that

$f(m,n) = f(m',n') \quad (m, n, m', n'$ in $\omega$), that is,

$$(m+n)\cdot(m+n)+m = (m'+n')\cdot(m'+n')+m' \tag{1}$$

and prove

$$m = m' \wedge n = n' \tag{2}$$

Well, if $m+n = m'+n'$, then $m = m'$ from (1) by VI.10.11, and then $n = n'$.

We show that $m+n \neq m'+n'$ cannot apply; then we are done. So let instead $m+n < m'+n'$. Thus $m+n+1 \leq m'+n'$. It follows[†] that

$$(m+n)\cdot(m+n)+m+m+n+n+1 \leq (m'+n')\cdot(m'+n')$$

Hence

$$(m+n)\cdot(m+n)+m+m+n+n+1 \leq (m'+n')\cdot(m'+n')+m'$$

By (1) and VI.10.11 again, $m+n+n+1 \leq 0$, which is absurd.

Thus the inverse relation $f^{-1} : \omega \to \omega^2$ is a (nontotal) onto *function*. By VII.2.6, $\omega^2$ is countable. Since it is infinite,[‡] it is enumerable.

**VII.2.10 Corollary.** *$\omega \sim \omega^n$ for $n \geq 2$.*

*Proof.* $\omega^{n+1} = \omega^n \times \omega$. Now use induction on $n$ in $\omega - \{0, 1\}$, and VII.2.9. □

We can also view the above as a theorem schema (one theorem for each $n \in \mathbb{N}$, rather than the single theorem $(\forall n \in \omega)(n \geq 2 \to \omega \sim \omega^n)$) and prove it by informal induction on $\mathbb{N} - \{0, 1\}$.

**VII.2.11 Proposition.** *If $A_i$ is countable for $i = 1, \ldots, n$, then so is $\bigtimes_{i=1}^{n} A_i$.*

Theorem schema.

*Proof.* Let $f_i : \omega \to A_i$ be onto for $i = 1, \ldots, n$. Then $\langle f_1, \ldots, f_n \rangle : \omega^n \to \bigtimes_{i=1}^{n} A_i$ is onto, where $\langle f_1, \ldots, f_n \rangle$ denotes the function $\lambda \vec{x}_n . \langle f_1(x_1), \ldots, f_n(x_n) \rangle$.

[†] By “squaring”. We are using the distributive law and commutativity of + and $\cdot$ on $\omega$ freely – cf. VI.10.19($iv$).

[‡] $\omega^2 \supseteq \{0\} \times \omega \sim \omega$, the $\sim$ obtained via $\langle 0, n \rangle \to n$ (cf. Exercise VII.2).

To conclude, we need an onto function $g : \omega \to \omega^n$, since $\langle f_1, \ldots, f_n \rangle \circ g : \omega \to \bigtimes_{i=1}^{n} A_i$ will then be onto. This we have by VII.2.10. □

*Informally*, using $\mathbb{N}$ for $\omega$, one can conclude the above argument in this alternative manner (without invoking VII.2.10): Let

$$h = \lambda \vec{x}_n . p_1^{x_1+1} p_2^{x_2+1} \cdots p_n^{x_n+1}$$

where $p_i$ is the $i$th prime ($p_0 = 2, p_1 = 3, p_2 = 5, \ldots$). By the (informal) prime factorization theorem, $h : \mathbb{N}^n \to \mathbb{N}$ is 1-1. Trivially, it is also total. Thus if $g = h^{-1}$, the inverse relation, $g : \mathbb{N} \to \mathbb{N}^n$ is an onto function.

Of course, armed with sufficient strength of will (and time and space), one can develop the properties of the formal natural numbers to the point that one proves the prime factorization theorem within ZFC (ZF suffices, actually). Then one can turn the above informal reasoning fragment to a formal one.

**VII.2.12 Proposition.** *If, for $i = 1, \ldots, n$, $A_i$ is countable, then so is $\bigcup_{i=1}^{n} A_i$.*

The above is stated as a schema, one theorem for each $n \in \mathbb{N}$. A formal version uses a function $f$ with $\mathrm{dom}(f) = \omega$. It takes the form

$$(\forall n \in \omega)\Big((\forall i \in n) f(i) \sim \omega \to \bigcup \{f(i) : i \in n\} \sim \omega\Big)$$

and is proved pretty much like the schema version.

*Proof.* Let $f_i : \omega \to A_i$ be onto for $i = 1, \ldots, n$. Define $g : \omega \times \omega \to \bigcup_{i=1}^{n} A_i$ by $g(i, x) = f_i(x)$ for all $x \in \omega$ and $i = 1, \ldots, n$. Clearly, $g$ is onto, for if $a \in \bigcup_{i=1}^{n} A_i$, then, say, $a \in A_m$ for some $m$. By ontoness of $f_m$, there is an $x \in \omega$ such that $f_m(x) = a$, that is, $g(m, x) = a$. Now invoke VII.2.6 and VII.2.9. □

We observe that the $g$ of the previous proof is not total.

**VII.2.13 Theorem (A Countable Union of Countable Sets Is Countable).** *If, for all $i \in \omega$, $A_i$ is countable, then so is $\bigcup_{i=0}^{\infty} A_i$.*

*Proof.* Let $f_i : \omega \to A_i$ be onto for all $i \in \omega$. Define $g$ on $\omega \times \omega$ as in the previous proof, and proceed in an identical fashion. □

**VII.2.14 Remark.** (1) The nickname of the theorem has the obvious justification as the family $(A_i)_{i \in \omega}$ is countable, indeed enumerable.

(2) The proof of Theorem VII.2.13 involved (tacitly) the axiom of choice. This happened during the definition of $g$, where one out of, possibly, several $f_i$ was (tacitly) chosen for each $i \in \omega$. The omitted details are as follows:

Since $\{f : f : \omega \to A_i \text{ is onto}\} \neq \emptyset$ for $i \in \omega$, there is an $h$ in $\prod_{i \in \omega}\{f : f : \omega \to A_i \text{ is onto}\}$. For each $i \in \omega$, $h(i)$ is the $f_i$ used in the proof.

Was this a peculiarity of this particular proof? No, as a result of Feferman and Levy (1963) shows: without the axiom of choice we may have a countable union of countable sets that turns out to be *uncountable*.

(3) The axiom of choice is provable for finite sets of sets, as we already know. Thus to construct $g$ in the proof of Proposition VII.2.12 we did not need AC to select one (out of the possibly many) $f_i$ for each $i = 1, \ldots, n$.

(4) In each of the results VII.2.11, VII.2.12, and VII.2.13, if any of the $A_i$ is enumerable, then so are

$$\bigtimes_{i=1}^{n} A_i, \quad \bigcup_{i=1}^{n} A_i, \quad \text{and} \quad \bigcup_{i=0}^{\infty} A_i$$

For the case of $\bigcup$ this follows from VII.1.10; for the other case see Exercise VII.15.

**VII.2.15 Example.** $\bigcup_{n=1}^{\infty} \omega^n$ is enumerable by Theorem VII.2.13, Corollary VII.2.10, and Remark VII.2.14(4). A direct proof – assuming an undertaking to develop enough arithmetic in ZF – bypasses the axiom of choice in this special case.

Let $f(x) = \langle x_0, \ldots, x_m \rangle$ whenever $x = p_0^{x_0+1} p_1^{x_1+1} \cdots p_m^{x_m+1}$. By the prime factorization theorem, this leads to an onto (but nontotal) function $f : \omega \to \bigcup_{n=1}^{\infty} \omega^n$. □

**VII.2.16 Example (Informal).** Let us see that $A \cup B$ is countable whenever $A$ and $B$ are, this time using an elementary (*informal*) technique traceable back to Cantor, rather than observing that this statement is a special case of Proposition VII.2.12.

According to hypothesis (see the discussion following Corollary VII.2.6), $A$ is enumerated (possibly with repetitions) as

$$a_0, a_1, a_2, \ldots$$

and $B$ is enumerated as

$$b_0, b_1, b_2, \ldots$$

Following the arrows in the diagram below, we trace an enumeration of $A \cup B$:

$$\begin{array}{cccccccc}
a_0 & & a_1 & & a_2 & & a_3 & \ldots \\
\downarrow & \nearrow & \downarrow & \nearrow & \downarrow & \nearrow & \downarrow & \ldots \\
b_0 & & b_1 & & b_2 & & b_3 & \ldots
\end{array}$$

□

**VII.2.17 Example (Informal).** We present an informal proof that $\omega^2$ is enumerable by providing an enumeration diagrammatically, as in the previous example:

$$\begin{array}{cccccccc}
\langle 0, 0\rangle & & \langle 0, 1\rangle & & \langle 0, 2\rangle & & \langle 0, 3\rangle & \cdots \\
 & \nearrow & & \nearrow & & \nearrow & & \\
\langle 1, 0\rangle & & \langle 1, 1\rangle & & \langle 1, 2\rangle & & & \\
 & \nearrow & & \nearrow & & & & \\
\langle 2, 0\rangle & & \langle 2, 1\rangle & & & & & \\
 & \nearrow & & & & & & \\
\langle 3, 0\rangle & & & & & & & \\
\vdots & & & & & & &
\end{array}$$

□

**VII.2.18 Example (Informal).** It is easy to see that the set of integers, $\mathbb{Z} = \{\ldots, -1, 0, 1, \ldots\}$, is enumerable. One way to do this is to observe first that $\lambda x. - x$ is a 1-1 correspondence between (the real) $\omega$ (if you prefer, you may use the real alternative, $\mathbb{N}$) and $\{\ldots, -1, 0\}$, the non-positive numbers $\mathbb{NP}$. Then observe that $\mathbb{Z} = \mathbb{NP} \cup \omega$, and invoke either Proposition VII.2.12 or Example VII.2.16.

Another way to do the same is to view $\mathbb{Z}$ as $\{0, 1\} \times \mathbb{N}$ (or $\{0, 1\} \times \omega$, using the real $\omega$), where $\langle 0, n\rangle$ stands for $n \in \mathbb{N}$, whereas $\langle 1, n\rangle$ stands for $-n$ for $n \in \mathbb{N}$. By Proposition VII.2.11 (see also Remark VII.2.14(4)), once again, $\mathbb{Z}$ is enumerable. □

**VII.2.19 Example (Informal).** We next see that $\mathbb{Q}$, the set of rational numbers, is enumerable.

This may appear, at first sight, surprising, because of the *density* of rational numbers: Between any two rational numbers $r$ and $s$ there is another rational number, for example, $(r + s)/2$. Thus, intuitively, there seem to be "more" numbers in $\mathbb{Q}$ than in $\mathbb{N}$ (which does not enjoy a density property). Well, intuition can be wrong in connection with the cardinality of infinite sets. (We will see another counterintuitive result in Section VII.4, namely, that there are as many reals in the unit square, $[0, 1]^2$, as there are in the unit segment, $[0, 1]$. See also Exercise VII.35.)

The justification of the claim is straightforward:

$$\mathbb{Q} = \{m/n : m \in \mathbb{Z} \wedge n \in \mathbb{N} - \{0\}\} \tag{1}$$

Since $\mathbb{N} \sim \mathbb{N} - \{0\}$ via $\lambda x.x + 1$,

$$\mathbb{Z} \times (\mathbb{N} - \{0\}) \sim \mathbb{N} \tag{2}$$

by Proposition VII.2.11 and Remark VII.2.14(4).

Since the function $\mathbb{Z} \times (\mathbb{N} - \{0\}) \to \mathbb{Q}$ given by $\langle m, n\rangle \mapsto m/n$ is onto, (2) and (1) yield an onto function $\mathbb{N} \to \mathbb{Q}$. □

**VII.2.20 Example (Informal).** Let us "count" the polynomials of one variable (say, $x$), with integer coefficients.

Such a polynomial is a function of $x$, whose value for each $x$ is given by the expression

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n, \quad \text{for short,} \quad \sum_{i=0}^{n} a_i x^i.$$

The $a_i$ are the *coefficients*, and, in this example, they are in $\mathbb{Z}$. Whenever $a_n \neq 0$, we say that the *degree* of the polynomial is $n$. We identify each $n$th-degree polynomial, $\sum_{i=0}^{n} a_i x^i$, with the $(n + 1)$-tuple $\langle a_0, \ldots, a_n\rangle$.

It follows that the set of $n$th-degree polynomials is $\mathbb{Z}^{n+1}$ and therefore the set of *all* polynomials is

$$\bigcup_{n=1}^{\infty} \mathbb{Z}^n$$

Since we already know that $\omega \sim \mathbb{Z}$ (Example VII.2.18), the set of polynomials is enumerable, by Example VII.2.15. (See also Exercises VII.26 and VII.27.) □

We now turn to a characterization of infinite sets due to Dedekind (1888).[†] This characterization is contained in the following definition.

**VII.2.21 Definition.** A set $A$ is *Dedekind-infinite* iff it is equinumerous with some of its *proper* subsets. Otherwise, it is *Dedekind-finite*. □

[†] This characterizing property of infinite sets was also observed by Cantor and Bolzano. See also Wilder (1963, p. 65).

**VII.2.22 Remark.** A set which is Dedekind-infinite is also infinite.

We prove the equivalent contrapositive statement, that if a set $A$ is finite in the "ordinary" sense (Definition VII.1.3), then it is also Dedekind-finite (i.e., *not* Dedekind infinite). Indeed, if $f : A \to n \in \omega$ is a 1-1 correspondence and if $B$ is any proper subset of $A$, then

(1) $B \sim f[B]$, and
(2) $f[B] \subset n$.

By Corollary VII.1.7, $f[B] \not\sim n$; hence $f[B] \not\sim A$. By (1), $B \not\sim A$. Since $B$ was an *arbitrary* proper subset of $A$, our conclusion is that $A$ is not Dedekind-infinite.

In what follows we will show the equivalence of the two definitions of finite (or infinite). □

*For the balance of this discussion, "infinite" and "finite", without the qualification "Dedekind", refer to the ordinary notions, as per Definition VII.1.3.*

**VII.2.23 Lemma.** *Every infinite set has an enumerable subset.*

*Proof.* Let $A$ be infinite. By VI.5.54, there is an $\alpha$ and a 1-1 correspondence $f : \alpha \to A$. By Exercise VII.2, $\alpha$ is infinite; hence $\omega \leq \alpha$, i.e., $\omega \subseteq \alpha$ (otherwise, $\alpha < \omega$, whence $\alpha$ is a natural number and therefore finite).

The set $f[\omega]$, being an enumerable subset of $A$, settles the issue. □

**VII.2.24 Lemma.** *If $A$ is infinite and $B$ is countable, then $A \cup B \sim A$.*

*Proof.* Let $C = B - A$, and $D$ be an enumerable subset of $A$.

By Example VII.2.8, $C$ is countable. Thus $D \cup C \sim D$ (see Remark VII.2.14(4)). Extend the above 1-1 correspondence to one between $A \cup B$ and $A$, as follows: Let each $x \in A - D$ correspond to itself, and observe that $A \cap C = \emptyset$, $A \cup B = A \cup C = (A - D) \cup (D \cup C)$, and $A = (A - D) \cup D$. □

**VII.2.25 Theorem.** *The notions "infinite" and "Dedekind infinite" are equivalent.*

*Proof.* That Dedekind infinite implies infinite is the content of Remark VII.2.22. So let next $A$ be infinite.

*Case 1.* There is a 1-1 correspondence $f : \omega \to A$, i.e., $A$ is enumerable. From $\omega \sim \omega - \{0\}$ (via $x \mapsto x + 1$) it follows that $f[\omega - \{0\}] \sim A$; moreover, $f[\omega - \{0\}] \subset A$.

*Case 2.* $A$ is not enumerable. By Lemma VII.2.23, $A$ has an enumerable subset $B$. By Exercise VII.16, $A - B$ is infinite (otherwise $A = (A - B) \cup B$ is enumerable). By Lemma VII.2.24, $A \sim A - B$. □

In the next section, among other things, we see that case 2 above is not vacuous.

## VII.3. Diagonalization; Uncountable Sets

In this section we study the important technique of *diagonalization* through several examples. It was devised by Cantor in order to prove that the set of real numbers is uncountable, and it has since found many applications in logic, such as in the proof of Gödel's incompleteness theorems and later in recursion theory (and its offspring, computational complexity). To a large extent, recursion theory and complexity theory are the art and science of diagonalization.

Described generally, given a "square table" (that is, a total function $\mathbb{F} : \mathbb{A} \times \mathbb{A} \to \mathbb{X}$), this method defines an $\mathbb{A}$-long *array* of elements of $\mathbb{X}$ (that is, a function $\mathbb{D} : \mathbb{A} \to \mathbb{X}$) that is different from *all* the "rows" of the table (where the $h$th "row" of $\mathbb{F}$ is the function $\mathbb{H} = \lambda x.\mathbb{F}(h, x)$). The idea, due to Cantor, can be described like this:

Start with the function $\lambda x.\mathbb{F}(x, x)$ (the "main diagonal" of the table). If this were to be the *same* as the $h$th row, then, in particular, $\mathbb{H}(h) = \mathbb{F}(h, h)$.[†]

Suppose now that we want to build an $\mathbb{A}$-long array that *cannot* equal the $h$th row. It suffices to take a *modified* diagonal: Just change the entry $\mathbb{F}(h, h)$.

It is clear now what needs to be done to get an $\mathbb{A}$-long array $\mathbb{D}$ that fits *nowhere* as a row. Take, again, the diagonal, but change *every one* of its entries. That is,

$$\mathbb{D}(x) = \text{some element in } \mathbb{X} - \{\mathbb{F}(x, x)\} \tag{1}$$

Clearly this works, i.e., for each $a \in \mathbb{A}$, $\mathbb{D} \neq \lambda y.\mathbb{F}(a, y)$; for (1) yields $\mathbb{D}(a) \neq \mathbb{F}(a, a)$.

We will illustrate the above general description of diagonalization in the following examples.

**VII.3.1 Example.** Let $(f_n)_{n \in \omega}$ be a countable family of total functions $f_n : \omega \to \omega$.

[†] Intuitively, the main diagonal was "rotated" counterclockwise, by 45 degrees, around the *pivot* entry $\mathbb{F}(h, h)$.

The function $d = \lambda x.f_x(x) + 1$ is different from each $f_x$ at input $x$; thus $d$ does not belong to the family. Let us verify: If $d = f_i$ for some $i \in \omega$, then $d(i) = f_i(i)$. On the other hand, by the definition of $d$, $d(i) = f_i(i) + 1$.

We conclude that $f_i(i) = f_i(i) + 1$, a contradiction, since both sides of "=" are defined.[†]

Finally, we note that the argument just presented indeed fits the general description of diagonalization. Here the "table" is $F = \lambda mn.f_m(n)$, and one particular way to build $\mathbb{D}$ of (1) (here called "$d$") is to make $d(x)$ different from $f(x, x)$ by adding 1 to the latter.

$d(x) = f_x(x) + x + 1$ would have worked too. □

**VII.3.2 Proposition.** *The set $A = {}^{\omega}\omega$ is uncountable.*

Recall that ${}^{X}Y$ is the set of all total functions $X \to Y$.

*Proof.* If $A$ were countable, then there would be an enumeration $(f_n)_{n\in\omega}$ of all its members. Example VII.3.1 shows that this is impossible, as any such (attempted) enumeration will omit at least one member of $A$, for example $d$. □

**VII.3.3 Corollary.** *The set ${}^{\omega}2$ is uncountable.*

*Proof.* Exercise VII.30. □

**VII.3.4 Example (Informal).** Diagonalization is often applied to define a *class* that does *not* belong to an indexed family of classes $(\mathbb{P}\langle x\rangle)_{x\in\mathbb{J}}$, where $\mathbb{J}$ is a class and $\mathbb{P}$ a relation on $\mathbb{J}$ (we are speaking informally, ignoring issues of left-narrowness). This is done by defining the "diagonal class" $\mathbb{E}$, setting

$$\mathbb{E} = \{x \in \mathbb{J} : x \notin \mathbb{P}\langle x\rangle\} \tag{1}$$

or

$$\mathbb{E} = \{x \in \mathbb{J} : x \not\!\mathbb{P}\, x\} \tag{1$'$}$$

Clearly this works, i.e., $\mathbb{E} \neq \mathbb{P}\langle x\rangle$ for all $x \in \mathbb{J}$, for if

$$\mathbb{E} = \mathbb{P}\langle a\rangle \qquad \text{for some } a \in \mathbb{J} \tag{2}$$

[†] Clearly, this argument breaks down if the family $(f_n)_{n\in\omega}$ contains nontotal functions, in which case we employ Kleene's weak equality $\simeq$. Then it is possible to have $f_i(i) \uparrow$, in which case $f_i(i) \simeq f_i(i) + 1$.

then

$$a \in \mathbb{P}\langle a\rangle \overset{\text{by (2)}}{\longleftrightarrow} a \in \mathbb{E} \overset{\text{by (1)}}{\longleftrightarrow} a \notin \mathbb{P}\langle a\rangle$$

– a contradiction.

This is not a new flavour of diagonalization, but fits under the general discussion on p. 451 above. Indeed, think of the "table" $\mathbb{F} : \mathbb{J} \times \mathbb{J} \to 2$ defined by[†]

$$\mathbb{F}(x, y) = \begin{cases} 0 & \text{if } x \,\mathbb{P}\, y \\ 1 & \text{otherwise} \end{cases}$$

The general discussion would lead to the "diagonal object"

$$\mathbb{D} = \lambda x.1 - \mathbb{F}(x, x) \tag{3}$$

which is a $\mathbb{J}$-long 0-1-valued array that cannot be a row of the "table". "$\mathbb{D}$" is just another way of saying "$\mathbb{E}$", for the former is the characteristic function of the latter, as the following equivalences show (for $x \in \mathbb{J}$):

$$\mathbb{D}(x) = 0 \leftrightarrow \mathbb{F}(x, x) = 1 \leftrightarrow x \not{\mathbb{P}} x \leftrightarrow x \in \mathbb{E}$$

As an application, let us look at the family $(x)_{x \in \mathbb{S}}$, where $\mathbb{S}$ is any *class* of sets. Here $\mathbb{J} = \mathbb{S}$ and $\mathbb{P}$ is the identity. Let $\mathbb{D} = \{x \in \mathbb{S} : x \notin x\}$, i.e., $x \in \mathbb{D}$ iff $x \in \mathbb{S} \wedge x \notin x$. Thus $\mathbb{D}$ behaves at $x$ differently than $x$ at $x$, and therefore it is not one of the $x$'s; in other words, $\mathbb{D} \notin \mathbb{S}$ (this is so because this diagonalization tells us that $\mathbb{D}$ is not in the family $(x)_{x \in \mathbb{S}}$, but this family equals $\mathbb{S}$).

So, by diagonalization, we have obtained an object not in $\mathbb{S}$. If we now let $\mathbb{S}$ be $\mathbb{V}_M$, the class of all sets, then $\mathbb{D}$ is the Russell class, and the above argument establishes (once again), that $\mathbb{D} \notin \mathbb{V}_M$, i.e., that $\mathbb{D}$ is not a set. Therefore, Russell's proof was a diagonalization over *all* sets to obtain an object which is not a set, and while ingenious and elegantly simple, the technique was borrowed from Cantor's work. □

With practice, one can expand the applicability of diagonalization to more general situations – for example, cases where we apply some transformation (function) to one of the table "coordinates". Say, given $\mathbb{P}$ and $\mathbb{J}$ as in VII.3.4, if $\mathbb{G} : \mathbb{J} \to \mathbb{J}$ is a function, then the class $\widetilde{\mathbb{E}} = \{\mathbb{G}(x) \in \mathbb{J} : \mathbb{G}(x) \notin \mathbb{P}\langle x\rangle\}$ is different from all $\mathbb{P}\langle x\rangle$ $(x \in \mathbb{J})$. Similarly, if $f : \omega \to {}^{\omega}\omega$ is an enumeration of total functions $\omega \to \omega$, then $d = \lambda x.f(x)(x) + 1$ is not in the range of $f$

[†] $\mathbb{F}$ is the characteristic function of $\mathbb{P}$.

(otherwise, $d = f(a)$ for some $a$ – hence $d(a) = f(a)(a)$ – but also $d(a) = f(a)(a) + 1$).[†]

**VII.3.5 Example (Informal).** Throughout, $[0, 1]$ will denote the real closed interval, $\{x \in \mathbb{R} : 0 \leq x \leq 1\}$. Since $\mathbb{Q}$, the set of rational numbers, is enumerable, then so is $[0, 1] \cap \mathbb{Q} = \{x \in \mathbb{Q} : 0 \leq x \leq 1\}$ (see Example VII.2.7). Now each rational in $[0, 1]$ has a decimal expansion $0.a_0 a_1 \ldots a_i \ldots$. For example,

$$1 = 0.\underbrace{99\ldots}_{\text{all 9's}},\ 0 = 0.\underbrace{00\ldots}_{\text{all 0's}},\ 1/3 = 0.\underbrace{33\ldots}_{\text{all 3's}}$$

and

$$1/2 = 0.5\underbrace{00\ldots}_{\text{all 0's}} \qquad \text{but also} \quad 1/2 = 0.4\underbrace{99\ldots}_{\text{all 9's}}$$

We next claim that the *set of all decimal expansions* of rationals in $[0, 1]$ is enumerable. Indeed, this set equals $\mathbb{Q}_{\text{inf}} \cup \mathbb{Q}_{\text{fin}}$, where $\mathbb{Q}_{\text{inf}}$ is the set of all *infinite* representations such as $0.33\ldots$, $0.99\ldots$, $0.499\ldots$, whereas $\mathbb{Q}_{\text{fin}}$ is the set of all *finite* representations, i.e., those that terminate with an infinite sequence of 0's, such as

$$0.\underbrace{00\ldots}_{\text{all 0's}} \quad \text{and} \quad 0.5\underbrace{00\ldots}_{\text{all 0's}}$$

Note that some rationals have both infinite and finite representations.

By Exercise VII.31, $\mathbb{Q}_{\text{inf}}$ is equinumerous to an infinite subset of $\mathbb{Q}$, and also $\mathbb{Q}_{\text{fin}}$ is equinumerous to an infinite subset of $\mathbb{Q}$; hence $\mathbb{Q}_{\text{inf}} \cup \mathbb{Q}_{\text{fin}} \sim \omega$, as required. So we have an enumeration $(0.a_0^n a_1^n \ldots a_i^n \ldots)_{n \in \omega}$ of all decimal expansions of the rational numbers in $[0, 1]$.

Consider the decimal expansion $d = 0.d^0 d^1 \ldots d^i \ldots$, where for all $i \in \omega$, $d^i \neq a_i^i$. For example, a well-defined way to achieve this is to set

$$d^i = \begin{cases} 2 & \text{if } a_i^i = 1 \\ 1 & \text{otherwise} \end{cases}$$

By diagonalization, $d$ does not belong to the family $(0.a_0^n a_1^n \ldots a_i^n \ldots)_{n \in \omega}$. Since the latter represents *all* the rationals in $[0, 1]$, and since $d$ represents a real in $[0, 1]$ it follows that $d$ is an *irrational* number in $[0, 1]$.

One can now continue to discover more irrationals in the interval by adding $d$ at the *beginning* of the enumeration and then diagonalizing again to obtain

[†] This type of argument shows, in recursion theory, that the set of *all* total computable functions cannot be "effectively" enumerated.

a *new* irrational $d'$ (each irrational has a unique expansion – infinite only). The reader may wish to refer to Wilder (1963, p. 89) to see a very interesting extension of this type of discussion. In particular, Wilder applies this type of diagonal technique to the set of algebraic numbers in [0, 1] to "construct" *transcendental*, i.e., non-algebraic, numbers (refer also to Exercise VII.27). □

**VII.3.6 Example (Informal: Cantor).** The set of real numbers in [0, 1] is uncountable.

Suppose instead that $[0, 1] \sim \omega$. Then, entirely analogously with Example VII.3.5, $[0, 1]_{\mathrm{fin}} \cup [0, 1]_{\mathrm{inf}} \sim \omega$, where $[0, 1]_{\mathrm{fin}}$ is the set of all *finite*, and $[0, 1]_{\mathrm{inf}}$ the set of all *infinite*, decimal expansions of reals in [0, 1], and therefore there is an enumeration $(0.a_0^n a_1^n \dots)_{n\in\omega}$ of the members of $[0, 1]_{\mathrm{fin}} \cup [0, 1]_{\mathrm{inf}}$.

However, the existence of the diagonal number $d$, defined as in Example VII.3.5, leads to a contradiction: On one hand $d$ cannot be in the enumeration. On the other hand,

$$d = 0.\underbrace{d^0 d^1 \dots}_{\text{1's and 2's}}$$

Hence it *is* in the enumeration. This contradiction establishes the claim. □

**VII.3.7 Proposition (Cantor).** *The set* $\mathbf{P}(\omega)$ *is uncountable.*

Contrast with Exercise VII.19.

*Proof.* Let us assume the contrary, i.e., that there is a 1-1 correspondence $f : \omega \to \mathbf{P}(\omega)$. Construct the diagonal set $D = \{x \in \omega : x \notin f(x)\}$.[†] Thus on one hand $D$ is not in the range of $f$; on the other hand it must be, since $D \subseteq \omega$. This contradiction establishes the claim. □

**VII.3.8 Example (Informal).** For the purpose of this example we will state without proof a few facts. To begin with, each real number $r$ in [0, 1] has a *binary* expansion, or can be represented in binary notation, as $r = 0.b_0 b_1 \dots b_i \dots$. This notation, or expansion, means (quite analogously with the familiar decimal case) that $r = \sum_{i=0}^{\infty} b_i/2^{i+1}$, where each $b_i$ is 0 or 1, and is called the $i$th *binary digit* or *bit*. An expansion $0.b_0 b_1 \dots b_i \dots$ is *finite* if for some $n$, $b_i = 0$ for all $i \geq n$; otherwise it is *infinite*. Infinite expansions are unique.

[†] To connect with the discussion on p. 451, here $\mathbb{P}$ on $\omega$ is given by $n \,\mathbb{P}\, m$ iff $n \in f(m)$; thus $\mathbb{P}\langle m \rangle = f(m)$.

Our purpose is to show that $[0, 1] \sim {}^{\omega}2 \sim \mathbf{P}(\omega)$. Indeed, to each $A \in \mathbf{P}(\omega)$ we associate its *characteristic function on* $\omega$, $\chi_A$, defined by

$$\chi_A(n) = \begin{cases} 0 & \text{if } n \in A \\ 1 & \text{otherwise} \end{cases}$$

It is clear that $A \mapsto \chi_A$ is a 1-1 correspondence from $\mathbf{P}(\omega)$ to ${}^{\omega}2$, which proves that the rightmost $\sim$ holds.

We next consider $[0, 1]_{\text{inf}}$ and $[0, 1]_{\text{fin}}$, the sets of all infinite and finite binary expansions, respectively, of *all* the reals in $[0, 1]$. For example,

$$0 = 0.\underbrace{00\ldots}_{\text{all 0's}}, \qquad 1 = 0.\underbrace{11\ldots}_{\text{all 1's}},$$

$$1/2 = 0.1\underbrace{00\ldots}_{\text{all 0's}} \qquad \text{but also} \quad 1/2 = .0\underbrace{11\ldots}_{\text{all 1's}}$$

Since the expansions in $[0, 1]_{\text{fin}}$ represent rationals (see Exercise VII.32), we have $[0, 1]_{\text{fin}} \sim \omega$ and therefore

$$[0, 1]_{\text{inf}} \sim [0, 1]_{\text{inf}} \cup [0, 1]_{\text{fin}} \tag{1}$$

by Lemma VII.2.24. Since every non-zero real has a unique infinite binary expansion (see also Exercise VII.33), (1) yields $(0, 1] \sim [0, 1]_{\text{inf}} \cup [0, 1]_{\text{fin}}$, and one more application of Lemma VII.2.24 ($[0, 1] \sim (0, 1]$) yields

$$[0, 1] \sim [0, 1]_{\text{inf}} \cup [0, 1]_{\text{fin}}$$

To conclude, observe that $f \mapsto 0.f(0)f(1)\ldots f(i)\ldots$ is a 1-1 correspondence ${}^{\omega}2 \to [0, 1]_{\text{inf}} \cup [0, 1]_{\text{fin}}$. □

**VII.3.9 Remark.** The technique of Example VII.3.8 showed that ${}^{x}2 \sim \mathbf{P}(x)$ for *any* set $x$. □

**VII.3.10 Theorem (Cantor's Theorem).** *For any set $x$, $x \not\sim \mathbf{P}(x)$.*

*Proof.* By contradiction, let there be a 1-1 correspondence $f : x \to \mathbf{P}(x)$. This leads to the family of sets $(f(a))_{a \in x}$, to which we can readily apply the technique of Proposition VII.3.7:

Let $D = \{a \in x : a \notin f(a)\}$. Thus $D \neq f(a)$ for all $a \in x$, yet $D \subseteq x$; thus it must be an $f(a)$ after all. This contradiction establishes the claim. □

We note that, relying on Example VII.3.8, we could have proved Cantor's theorem as follows: Let instead $x \sim \mathbf{P}(x)$. Then also $x \sim {}^{x}2$. So let $a \mapsto g_a$ be a 1-1 correspondence $x \rightarrow {}^{x}2$. The diagonal function $d = \lambda a.1 - g_a(a)$ is different from each $g_a$ (at $a$), yet it is a total 0-1-valued function on $x$, so it is a $g_a$. Contradiction.

The reader will recognize that the two arguments are essentially identical. Indeed, $d = \chi_D$.

**VII.3.11 Example (Informal).** We show here that $(-1, 1) \sim \mathbb{R}$, where $(-1, 1) = \{x \in \mathbb{R} : -1 < x < 1\}$. Indeed, let $f$ on $\mathbb{R}$ be defined by

$$f(x) = \frac{x}{1 + |x|}$$

Trivially, $f$ is total. Next, we see that it is 1-1. Indeed, let

$$\frac{a}{1 + |a|} = \frac{b}{1 + |b|} \tag{1}$$

where $a$ and $b$ are in $\mathbb{R}$. This leads to

$$a - b = b|a| - a|b| \tag{2}$$

By (1), $ab \geq 0$, so we analyze (2) under just two cases.

*Case 1:* $a \geq 0$ and $b \geq 0$. Then $a - b = ba - ab = 0$.
*Case 2:* $a \leq 0$ and $b \leq 0$. Then $a - b = -ba - (-ab) = 0$.

Both cases lead to $a = b$, so $f$ is 1-1.

Finally, $f$ is onto $(-1, 1)$. Indeed, let $c \in (-1, 1)$. The reader can easily verify that if $c = 0$, then $f(0) = c$; if $-1 < c < 0$, then $f(c/(1 + c)) = c$; if $0 < c < 1$, then $f(c/(1 - c)) = c$. □

## VII.4. Cardinals

In this section, following von Neumann, we assign a measure of cardinality to each set, its *cardinal number*.

At the very least, cardinal numbers must be $\sim$-invariants (i.e., equinumerous sets must measure identically). It is also desirable that this measure be consistent with the measures we have already accepted for the cardinality of finite sets, since the latter perfectly fit with our intuition.

The requirement that cardinal numbers be $\sim$-invariants means that for any set $A$, its cardinal number depends on the class of all sets equinumerous to

$A$ rather than just on $A$. It was therefore natural that, at first, mathematicians defined (Frege-Russell definition) the cardinal number of a set $A$ to be "the 'set' of all sets equinumerous to $A$". This, of course, eventually led to trouble because these cardinal numbers were "too big" to be sets. For example, the cardinal number of $\{\emptyset\}$ would be, according to this definition, the "set" of all singletons (one-element sets), but this "set" is in 1-1 correspondence with the class of all sets and urelements (via $x \mapsto \{x\}$) and therefore is *not* a set, by the collection axiom.

Thus cardinal numbers, as "defined" above, cannot be objects of study in our theory. However, in the old way of doing set theory (where *any* collection, in principle, was a set and therefore was entitled to be studied in the theory) there were still problems, as even cardinal numbers of singletons would be closely associated with the "self-contradictory notion" of the "set of all sets" (the reader, once again, is referred to the discussion in Wilder (1963, pp. 98–100)).

The way out this difficulty (von Neumann) is simple. Rather than take for the cardinal number of $A$ the class of all sets equinumerous to $A$, just take a "canonical" or "normalized" representative from this class (the terms in quotes mean that the representative ought not to depend too strongly on $A$ itself, so that $\sim$-invariance can be assured). By Zermelo's theorem (VI.5.54), each such class contains ordinals; so take the least such ordinal to measure the cardinality.

**VII.4.1 Definition.** For any set $x$, its *cardinal number*, or *cardinality*, is defined to be $\min\{\alpha : \alpha \sim x\}$ and is denoted by $\mathrm{Card}(x)$. Cardinal numbers are also simply referred to as *cardinals*. Thus a cardinal is just the cardinal number of some set.

We shall use (in *argot*) lowercase fraktur letters to denote arbitrary cardinals, i.e., cardinal-typed variables (e.g., $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{m}$), but also lowercase Greek letters around the middle of the alphabet, typically, $\kappa$ and $\lambda$. The class of all cardinals will be denoted by Cn. □

By definition, $\mathrm{Cn} \subseteq \mathrm{On}$.

Here are some useful and immediate consequences.

**VII.4.2 Proposition.** *For any sets $x$ and $y$ the following hold:*

(a) $x \sim \mathrm{Card}(x)$.
(b) $x \sim y$ *iff* $\mathrm{Card}(x) = \mathrm{Card}(y)$.

*Proof.* Part (a) follows immediately from the definition.

For (b), assume $x \sim y$. Then $\mathrm{Card}(x) = \min\{\alpha : \alpha \sim x\} = \min\{\alpha : \alpha \sim y\} = \mathrm{Card}(y)$. This settles the only-if part. For the if part, use (a) to write $x \sim \mathrm{Card}(x) = \mathrm{Card}(y) \sim y$. □

Part (b) shows that Card() is a $\sim$-invariant.

**VII.4.3 Proposition.** *For any ordinal $\alpha$, $\alpha \in \mathrm{Cn}$ iff there is* no *$\beta < \alpha$ such that $\beta \sim \alpha$.*

*Proof.* Let $\alpha \in \mathrm{Cn}$ be due to $\alpha = \mathrm{Card}(x)$ for some set $x$. Consider the set (why *set*?) $S = \{\gamma : \gamma \sim x\}$. We have

$$\alpha = \min S \tag{1}$$

If some $\beta < \alpha$ satisfies $\beta \sim \alpha$, then this contradicts (1), since $\beta \in S$. This argument establishes the only-if part.

For the if part, let there be no $\beta < \alpha$ such that $\beta \sim \alpha$. Then $\alpha$ is smallest in $\{\gamma : \gamma \sim \alpha\}$, i.e., $\alpha = \mathrm{Card}(\alpha)$ and therefore $\alpha \in \mathrm{Cn}$. □

Proposition VII.4.3 gives a characterization of cardinals which is independent of the sets whose cardinality these cardinals measure. It is helpful in showing that specific ordinals are cardinals. Because of the proposition, cardinals are also called *initial ordinals*.

**VII.4.4 Example.** Every natural number, i.e., finite ordinal, is a cardinal.

Indeed, by Corollary VII.1.8 we obtain that $\alpha \not\sim \beta$ whenever $\alpha \in \beta \in \omega$. Therefore, fixing attention on $\beta$, it is a cardinal by Proposition VII.4.3.

It follows that $\beta = \mathrm{Card}(\beta)$, but then (Definition VII.1.3) $\mathrm{Card}(\beta) = |\beta|$, so that the definition of cardinals for finite sets is indeed a special case of Definition VII.4.1, as we hoped it would be. □

So far we have obtained that $\mathrm{Cn} \neq \emptyset$, in particular, $\omega \subseteq \mathrm{Cn}$.

**VII.4.5 Example.** We now establish that $\omega \in \mathrm{Cn}$. Indeed, just invoke Proposition VII.1.13 to see that $\alpha \in \omega$ implies $\alpha \not\sim \omega$. □

We have just witnessed that $\omega$ is the smallest infinite cardinal (i.e., smallest infinite ordinal that is a cardinal). Definitions VII.1.3 and VII.2.1 are also worth restating in the present context: $x$ is finite iff $\mathrm{Card}(x) < \omega$; it is enumerable iff $\mathrm{Card}(x) = \omega$; it is countable iff $\mathrm{Card}(x) \le \omega$; it is uncountable iff $\mathrm{Card}(x) > \omega$.

**VII.4.6 Proposition.** *For any ordinal $\alpha$,*

(i) $\mathrm{Card}(\alpha) \le \alpha$,
(ii) $\mathrm{Card}(\alpha) = \alpha$ *iff* $\alpha \in \mathrm{Cn}$.

*Proof.* (i): $\mathrm{Card}(\alpha) = \min S$, where $S = \{\gamma : \gamma \sim \alpha\}$. But $\alpha \in S$.

(ii): *If part.* Let $\alpha \in \mathrm{Cn}$. If $\mathrm{Card}(\alpha) < \alpha$, then $\mathrm{Card}(\alpha) \sim \alpha$ contradicts Proposition VII.4.3.

*Only-if part.* Trivially, the hypothesis says "$\alpha$ is a cardinal". □

**VII.4.7 Example.** For any cardinal $\mathfrak{m}$, $\mathrm{Card}(\mathfrak{m}) = \mathfrak{m}$. Indeed, this just rephrases Proposition VII.4.6(ii).

This observation is often usefully applied as $\mathrm{Card}(\mathrm{Card}(x)) = \mathrm{Card}(x)$, where $x$ is any set. □

**VII.4.8 Proposition.** *Every infinite cardinal is a limit ordinal.*

*Proof.* The claim is known to be true for $\omega$. So let $\omega < \mathfrak{a}$, and assume instead that $\mathfrak{a} = \beta + 1$ for some $\beta$. Now, $\beta$ is infinite; otherwise $\mathfrak{a} = \beta + 1 < \omega$.

By Lemma VII.2.24, $\beta \cup \{\beta\} \sim \beta$; therefore $\mathfrak{a} \sim \beta$, which along with $\beta < \mathfrak{a}$ contradicts that $\mathfrak{a}$ is a cardinal. □

The above result shows that there are many "more" ordinals than cardinals. For example, $\omega + 1$, $\omega + 2$, and $\omega + i$ for any $i \in \omega$ are not cardinals.

It also suggests the question of whether indeed there are *any* cardinals above $\omega$. This question will be eventually answered affirmatively. As a matter of fact, there are so many cardinals that Cn is a proper class.

The following result is very important for the further development of the theory of cardinal numbers.

**VII.4.9 Theorem.** *For any sets $A$ and $B$, $A \subseteq B$ implies that* $\mathrm{Card}(A) \le \mathrm{Card}(B)$.

*Proof.* Let $\mathfrak{b} = \mathrm{Card}(B)$ and $f : B \to \mathfrak{b}$ be a 1-1 correspondence. Define $<$ on $B$ by

$$x < y \quad \text{iff} \quad f(x) \in f(y) \tag{1}$$

By VI.3.12, $<$ well-orders $B$ and hence $A$. Let $\alpha = \text{ran}(\phi)$, where $\phi$ on $A$ is given by the inductive definition

$$\phi(y) = \{\phi(x) : x < y \wedge x \in A\} \tag{2}$$

We know (VI.4.32) that $\text{ran}(\phi) \in \text{On}$ (which justifies calling it "$\alpha$") and that $\phi(x) \in \text{On}$ for all $x \in A$.

We next show that

$$\text{for all } x \in A, \qquad \phi(x) \subseteq f(x) \tag{3}$$

We do so by induction over $A$ with respect to $<$. So assume (3) for all $x$ in $A$ such that $x < y \in A$ (this is the I.H.), and prove it for $y$. Now if $y$ is minimum in $A$ (basis), then $\phi(y) = \emptyset$, from which the claim follows in this case. Let then $y$ be non-minimum and $z \in \phi(y)$. It follows from (2) that $z = \phi(x)$ for some $x \in A$ where $x < y$. By the I.H. $z \subseteq f(x) \in f(y)$ ((1) contributes "$\in$"), and since $f(x)$ and $f(y)$ are ordinals (being members of $\mathfrak{b}$), we obtain $z \in f(y)$, which concludes the inductive proof of (3).

We next observe that $\alpha \leq \mathfrak{b}$, i.e., $\alpha \subseteq \mathfrak{b}$. Indeed, let $\gamma \in \alpha$. Then $\gamma = \phi(x)$ for some $x \in A$, so that $\gamma \leq f(x)$ by (3). Since $f(x) \in \mathfrak{b}$, i.e., $f(x) < \mathfrak{b}$, we get $\gamma <$ (i.e., $\in$)$\mathfrak{b}$.

This last result, along with Propositions VII.4.2 and VII.4.6, yields $\text{Card}(A) = \text{Card}(\alpha) \leq \alpha \leq \mathfrak{b} = \text{Card}(B)$. □

The above theorem will provide the basic tools to compare cardinalities of sets. To this end we introduce a definition.

**VII.4.10 Definition.** For two sets $A$ and $B$, $A \preccurlyeq B$ means that there is a total and 1-1 $f : A \to B$. □

Intuitively, whenever $A \preccurlyeq B$, $B$ has at least as many elements as $A$. We will indeed see in VII.4.14 that $\text{Card}(A) \leq \text{Card}(B)$ is derivable under the circumstances. Let us, however, first state some trivial but useful observations.

**VII.4.11 Proposition.**

(i) $\preccurlyeq$ *is reflexive and transitive.*
(ii) *If* $A \subseteq B$, *then* $A \preccurlyeq B$.
(iii) $A \preccurlyeq B$ *iff for some* $C \subseteq B \;\; A \sim C$.
(iv) *If* $A \sim B$, *then* $A \preccurlyeq B$.

*Proof.* Exercise VII.37. □

**VII.4.12 Example.** Case (iv) in Proposition VII.4.11 cannot be improved to "iff". For example, $x \mapsto \{x\}$ establishes $a \preccurlyeq \mathbf{P}(a)$ for any set $a$. We know however that $a \not\sim \mathbf{P}(a)$ by Cantor's theorem (VII.3.10). This motivates the following definition. □

**VII.4.13 Definition.** If $A \preccurlyeq B$ but $A \not\sim B$, then we write $A \prec B$. □

**VII.4.14 Proposition.** *For any sets $A \neq \emptyset$ and $B$, the following are equivalent:*

(i) $A \preccurlyeq B$.
(ii) *There is an onto function $f : B \to A$.*
(iii) $\mathrm{Card}(A) \leq \mathrm{Card}(B)$.

*Proof.* The equivalence of (i) and (ii) follows directly from V.3.9. Next, let us assume (i) and prove (iii). By Proposition VII.4.11(iii), $A \sim C \subseteq B$ for some $C$. Hence, using Propositions VII.4.2 and VII.4.9, $\mathrm{Card}(A) = \mathrm{Card}(C) \leq \mathrm{Card}(B)$. Conversely, assume now (iii), i.e., $\mathrm{Card}(A) \subseteq \mathrm{Card}(B)$. The diagram below shows that $g \circ i \circ f : A \to B$ is total and 1-1, thus establishing (i), where $i : \mathrm{Card}(A) \to \mathrm{Card}(B)$ is the *inclusion map* $x \mapsto x$ and $f : A \to \mathrm{Card}(A)$ and $g : \mathrm{Card}(B) \to B$ are 1-1 correspondences:

$$\begin{tikzcd}
A \arrow[r, "g \circ i \circ f"] \arrow[d, "f"'] & B \\
\mathrm{Card}(A) \arrow[r, "i"'] & \mathrm{Card}(B) \arrow[u, "g"']
\end{tikzcd}$$

□

**VII.4.15 Corollary.** *For any sets $A$ and $B$, $A \prec B$ iff* $\mathrm{Card}(A) < \mathrm{Card}(B)$.

*Proof. If part.* The hypothesis yields $A \preccurlyeq B$ *and* $A \not\sim B$ (otherwise the cardinals of the two sets would be equal). Hence $A \prec B$.

*Only-if part.* The hypothesis yields $\mathrm{Card}(A) \leq \mathrm{Card}(B)$ *and* $\mathrm{Card}(A) \neq \mathrm{Card}(B)$. □

**VII.4.16 Corollary (Cantor).** *For any set $a$,* $\mathrm{Card}(a) < \mathrm{Card}(\mathbf{P}(a))$.

*Proof.* Indeed, $a \prec \mathbf{P}(a)$ by Example VII.4.12. □

By Corollary VII.4.16, there are infinitely many cardinals. Indeed, for any $\mathfrak{a}$, $\mathrm{Card}(\mathbf{P}(\mathfrak{a}))$ is a bigger cardinal. The preceding proposition relates comparisons of sets (as to size) with comparisons of their cardinal numbers and leads to the following important result, which has several names attached to it: Cantor, Dedekind, Schröder, and Bernstein.

**VII.4.17 Theorem (Cantor-Bernstein).** *For any sets $A$ and $B$, if $A \preccurlyeq B$* and *$B \preccurlyeq A$ then $A \sim B$ and conversely.*

*Proof.* The "conversely" part directly follows from Proposition VII.4.11. For the rest, observe that $A \preccurlyeq B$ and $B \preccurlyeq A$ yield $\mathrm{Card}(A) \leq \mathrm{Card}(B)$ and $\mathrm{Card}(B) \leq \mathrm{Card}(A)$ respectively, by Proposition VII.4.14; thus $\mathrm{Card}(A) = \mathrm{Card}(B)$. □

Our approach to cardinals relies on AC. Some authors define cardinal numbers in a way independent of AC (see, for example, Levy (1979)). In such an approach, there is a more obscure – but AC-free – proof[†] of the Cantor-Bernstein theorem, which we include here.

Let $f : A \to B$ and $g : B \to A$ be total and 1-1. We want to conclude that $A \sim B$.

Consider the operator $\Gamma$ over $A$ given by

$$\Gamma(S) = (A - g[B]) \cup g \circ f[S] \tag{1}$$

for all $S \subseteq A$. Clearly $\Gamma$ is monotone, so for some $X \subseteq A$ we have $\Gamma(X) = X$. (For example, $\overline{\Gamma}$ will do for $X$. You may want to review Theorem VII.1.27.) Set

$$X' = f[X] \tag{2}$$

$$Y = A - X \tag{3}$$

$$Y' = B - X' \tag{4}$$

so that

$$A = X \cup Y \quad \text{and} \quad X \cap Y = \emptyset \tag{5}$$

$$B = X' \cup Y' \quad \text{and} \quad X' \cap Y' = \emptyset \tag{6}$$

[†] Of course, AC enters via the Zermelo theorem in Definition VII.4.1 and in the proof of Theorem VII.4.9, on which the above-given proof of the Cantor-Bernstein theorem is based.

We will show that $Y = g[Y']$. Indeed,

$$\begin{aligned} g[Y'] &= g[B - X'] && \text{by (4)} \\ &= g[B] - g[X'] && \text{since } g \text{ is 1-1 and total} \\ &= g[B] - g \circ f[X] && \text{by (2)} \\ &= g[B] \cap (A - g \circ f[X]) && (7) \end{aligned}$$

By (7) and De Morgan's law, $A - g[Y'] = (A - g[B]) \cup g \circ f[X] = \Gamma(X) = X$. By (5), this is what we want.

To conclude, define $h : A \to B$ by

$$h(x) = \begin{cases} f(x) & \text{if } x \in X \\ g^{-1}(x) & \text{if } x \in Y \end{cases}$$

where $g^{-1} : \operatorname{ran}(g) \to B$ is, of course, a 1-1 correspondence. Clearly, $A \sim B$ via $h$. This concludes the AC-free proof.

**VII.4.18 Example (Informal).** *The self-contradictory notion of the "set of all sets".* Let us travel back to the point in time prior to the introduction of the axiomatic foundation of set theory. At that point *sets* and *classes* meant the same thing. The statement $x \in x$ was *not* necessarily false for all sets $x$; thus the notion of the set of all sets would not be disallowed via this route. Instead, a cardinality argument was then applied to show that the set of all sets could not possibly exist: Indeed, if $\mathbb{V}$ is the set of all sets, then $\mathbf{P}(\mathbb{V}) \subseteq \mathbb{V}$, therefore $\mathbf{P}(\mathbb{V}) \preccurlyeq \mathbb{V}$. Since also (VII.4.12) $\mathbb{V} \preccurlyeq \mathbf{P}(\mathbb{V})$, we get $\mathbb{V} \sim \mathbf{P}(\mathbb{V})$, contradicting Cantor's theorem. □

**VII.4.19 Example (Informal).** Let us see that $(0, 1] \times (0, 1] \sim (0, 1]$.

Indeed, $(0, 1]^2 \preccurlyeq (0, 1]$ via the function $\langle 0.a_0a_1 \ldots a_i \ldots, 0.b_0b_1 \ldots b_i \ldots \rangle \mapsto 0.a_0b_0a_1b_1 \ldots a_ib_i \ldots$, which is clearly total and 1-1 on the understanding that we only utilize infinite expansions. On the other hand, $(0, 1] \preccurlyeq (0, 1]^2$ via $x \mapsto \langle x, 1 \rangle$. The result follows from the Cantor-Bernstein theorem.

Compare the proof just given with the one you gave in Exercise VII.35. □

We next turn our attention to the transfinite sequence of cardinals.

**VII.4.20 Proposition.** *If $S$ is a set of cardinals, then $\bigcup S$ is a cardinal. Moreover, $\mathfrak{a} \leq \bigcup S$ for all $\mathfrak{a} \in S$.*

*Proof.* By VI.5.22, $\bigcup S$ is an ordinal. We show (see Proposition VII.4.6) that $\operatorname{Card}(\bigcup S) = \bigcup S$ by contradiction.

So let $\mathrm{Card}(\bigcup S) < \bigcup S$, i.e., $\mathrm{Card}(\bigcup S) \in \bigcup S$. By the definition of $\bigcup$,

$$\mathrm{Card}\left(\bigcup S\right) \in \mathfrak{a} \in S \quad \text{for some } \mathfrak{a} \tag{1}$$

and hence

$$\mathrm{Card}\left(\bigcup S\right) < \mathfrak{a} \subseteq \bigcup S \quad \text{for some } \mathfrak{a} \tag{2}$$

By Theorem VII.4.9, (2) yields a contradiction:

$$\mathrm{Card}\left(\bigcup S\right) < \mathfrak{a} \leq \mathrm{Card}\left(\bigcup S\right)$$

Finally, that $\mathfrak{a} \leq \bigcup S$ for all $\mathfrak{a} \in S$ follows from Theorem VI.5.22. □

**VII.4.21 Corollary.** Cn *is not a set.*

*Proof.* If it were a set, then $\mathfrak{a} = \bigcup \mathrm{Cn}$ for some $\mathfrak{a} \in \mathrm{Cn}$. But then $\mathfrak{a} < \mathrm{Card}(\mathbf{P}(\mathfrak{a})) \in \mathrm{Cn}$ contradicts the previous proposition (which yields $\mathrm{Card}(\mathbf{P}(\mathfrak{a})) \leq \bigcup \mathrm{Cn} = \mathfrak{a}$). □

**VII.4.22 Definition.** For any cardinal $\mathfrak{a}$, its *cardinal successor*, $\mathfrak{a}^+$, is the smallest cardinal $> \mathfrak{a}$. □

The above definition makes sense by Corollary VII.4.16 and the remark following it, since Cn is well-ordered by $<$ (i.e., $\in$). We can now define the alephs:

**VII.4.23 Definition.** The *aleph* transfinite sequence is given by the total function $\alpha \mapsto \aleph_\alpha$ on On defined inductively as follows:

$$\begin{aligned}
\aleph_0 &= \omega \\
\aleph_{\alpha+1} &= (\aleph_\alpha)^+ \\
\aleph_\alpha &= \bigcup\{\aleph_\beta : \beta < \alpha\} \qquad \text{if } \mathrm{Lim}(\alpha)
\end{aligned}$$

Each $\aleph_\alpha$ is an *aleph*.

A cardinal $\aleph_\alpha$ with $\mathrm{Lim}(\alpha)$ is called a *limit cardinal*, while one such as $\aleph_{\alpha+1}$ is called a *successor cardinal*. □

**VII.4.24 Remark.** (1) The reader will note that the term "limit cardinal" applies to the *index* of an infinite cardinal in the aleph sequence. It does *not* refer to the cardinal itself (all infinite cardinals are limit ordinals by VII.4.8).

(2) If $\mathrm{Lim}(\alpha)$, then $\aleph_\alpha = \bigcup\{\aleph_{\beta+1} : \beta < \alpha\}$. Indeed, by VII.4.20, $\bigcup\{\aleph_{\beta+1} : \beta < \alpha\}$ is a cardinal, say

$$\mathfrak{a} = \bigcup\{\aleph_{\beta+1} : \beta < \alpha\}$$

Since $\beta < \alpha$ implies $\beta + 1 < \alpha$, $\mathfrak{a} \le \aleph_\alpha$. On the other hand, $\gamma \in \aleph_\alpha$ implies that, for some $\beta < \alpha$, $\gamma \in \aleph_\beta$. But $\aleph_\beta < \aleph_{\beta+1}$ by definition, and $\aleph_{\beta+1}$ is transitive. Thus, $\gamma \in \aleph_{\beta+1} \subseteq \mathfrak{a}$. □

**VII.4.25 Proposition.** *The function $\alpha \mapsto \aleph_\alpha$ is strictly increasing.*

*Proof.* By definition, $\aleph_\alpha < \aleph_{\alpha+1}$. The result follows, by VI.5.38. □

In particular, $\alpha \mapsto \aleph_\alpha$ is normal.

The next theorem shows how to "compute" $\mathfrak{a}^+$.

**VII.4.26 Theorem.** *For all $\mathfrak{a}$, $\mathfrak{a}^+ = \{\alpha : \mathrm{Card}(\alpha) \le \mathfrak{a}\}$.*

*Proof.* Let us set $S = \{\alpha : \mathrm{Card}(\alpha) \le \mathfrak{a}\}$.

First, $S$ is transitive: Indeed, let $\alpha \in \beta \in S$. This yields $\alpha \subseteq \beta$; hence, $\mathrm{Card}(\alpha) \le \mathrm{Card}(\beta) \le \mathfrak{a}$, the last $\le$ by definition of $S$. Thus $\alpha \in S$.

Second, $S$ is a set: Indeed, if $\alpha \in S$, then $\alpha < \mathfrak{a}^+$, for otherwise $\mathfrak{a}^+ \le \mathrm{Card}(\alpha) \le \mathfrak{a}$. Therefore, $S \subseteq \mathfrak{a}^+$, and hence $S$ is a set. It follows that $S$ is an ordinal.

Let next, $\mathrm{Card}(S) \in S$. Then $\mathrm{Card}(\mathrm{Card}(S)) \le \mathfrak{a}$ and therefore $\mathrm{Card}(S) \le \mathfrak{a}$ (see VII.4.7) which yields $S \in S$, a contradiction.

Therefore $S$ is a cardinal. Clearly $\mathfrak{a} < S$, as the previous paragraph shows. By VII.4.22, $\mathfrak{a}^+ \le S$. □

By the previous theorem, $\aleph_1 = \{\alpha : \mathrm{Card}(\alpha) \le \omega\}$. That is, $\aleph_1$ is the set of all *countable ordinals*.

It is also noted that for each $\alpha$, $(\aleph_\alpha)^+ \le \mathrm{Card}(\mathbf{P}(\aleph_\alpha))$, since $\aleph_\alpha < \mathrm{Card}(\mathbf{P}(\aleph_\alpha))$ by Cantor's theorem, while $(\aleph_\alpha)^+$ is the smallest cardinal above $\aleph_\alpha$.

The conjecture (Hausdorff)

$$\aleph_{\alpha+1} = \mathrm{Card}(\mathbf{P}(\aleph_\alpha))$$

is the *generalized continuum hypothesis*, or GCH, whereas the special case conjectured by Cantor,

$$\aleph_1 = \mathrm{Card}(\mathbf{P}(\aleph_0)) \tag{1}$$

is the *continuum hypothesis*, or CH.

Gödel (1938, 1939, 1940) showed, using $\mathbb{L}$, that GCH is consistent with the Zermelo-Fraenkel ($+$AC) axioms of set theory, and Cohen (1963) showed that $\neg$GCH is also consistent with ZFC. Thus GCH is *independent* of the ZFC axioms; these axioms can neither prove it nor disprove it. So, as with AC, one can adopt either GCH or $\neg$GCH, as an axiom. This is not generally done, however. The other axioms of ZFC (including AC) are widely accepted as “really true”, being counterparts of reasonable principles (e.g., substitution, foundation), whereas our intuition does not help us at all to choose between GCH or $\neg$GCH. Our principles (or axioms) are not adequate to settle this question, and one hopes that additional intuitively “true” axioms will eventually be discovered and added which will settle GCH. It is noted that if one adopts GCH for the sake of experimentation, then several things become simpler in set theory (e.g., cardinal arithmetic – see Section VII.6), and even the axiom of choice becomes a theorem$^\dagger$ (the interested reader is referred to Levy (1979, p. 190)).

In the “real realm”, because $\mathbf{P}(\omega) \sim \mathbb{R}$ (by VII.3.8, VII.3.11, and Exercise VII.34), CH can be rephrased to read *there is no cardinal between $\omega$ and* Card($\mathbb{R}$), or also *every subset of $\mathbb{R}$ either has the cardinality of $\mathbb{R}$ or is countable.*

**Digression.** We briefly look into an alternative definition of cardinals, which is not based on the axiom of choice. This digression can be skipped without harm, as it is not needed for the rest of our development of set theory. Indeed, it is incompatible with Definition VII.4.1, which we are following (see Remark VII.4.28(3) below). Yet, the reader who is interested in foundational questions will find the material here illuminating.

**VII.4.27 Definition (Frege-Russell-Scott).** For any set $A$, its *cardinal number* or *cardinality*, in symbols Card($A$), is the class of all sets of *least rank* ($\rho$) equinumerous to $A$.

A *cardinal* is a class which is the cardinal number of some set. □

**VII.4.28 Remark.** (1) The above definition is essentially the original due to Frege and Russell suggested in the preamble to this section, where the “size” of cardinals has been drastically reduced down to set size (see VI.6.29). We state this as Proposition VII.4.29 below.

(2) The cardinal number of a set $A$ does not necessarily contain $A$ (i.e., cardinals of Definition VII.4.27 are not equivalence classes). To see this, look, for

$^\dagger$ For this to be non circular cardinals must be introduced in an AC-free manner. See the following **Digression**.

example, at $\mathrm{Card}(\{\omega\})$. By Proposition VI.6.21, $\rho(\omega)=\omega+1$; thus $\rho(\{\omega\})=\omega+2$ (VI.6.24).

Now let $a$ be any urelement. Then $\rho(\{a\})=1$ and $\{\omega\}\sim\{a\}$. Thus $\{a\}\in\mathrm{Card}(\{\omega\})$, but $\{\omega\}\notin\mathrm{Card}(\{\omega\})$.

(3) $\mathrm{Card}(\emptyset)=\{\emptyset\}$, an ordinal. However, if $x\neq\emptyset$ then $\emptyset\notin\mathrm{Card}(x)\neq\emptyset$, since $x\not\sim\emptyset$, i.e., cardinals of nonempty sets are *not* ordinals. □

**VII.4.29 Proposition.** *For any set $x$,* $\mathrm{Card}(x)$ *is a set.*

*Proof.* See VI.6.29. □

As before, Cn denotes the class of all cardinals.

**VII.4.30 Proposition.** *For any sets $x$ and $y$, $x\sim y$ iff* $\mathrm{Card}(x)=\mathrm{Card}(y)$.

*Proof. If part.* Let $a\in\mathrm{Card}(x)=\mathrm{Card}(y)$. Then $x\sim a\sim y$.

*Only-if part.* Directly from Definition VII.4.27. □

The above is the counterpart of Proposition VII.4.2(b), this time under Definition VII.4.27. It has been shown by Pincus (1974) that one cannot define "Card()" in ZF so that it satisfies $x\sim\mathrm{Card}(x)$ as well.

One now proceeds by adopting Definitions VII.4.10 and VII.4.13 for $\preccurlyeq$ and $\prec$. In particular, Proposition VII.4.11 is derivable. Next, $\leq$ on cardinals is *defined* through $\preccurlyeq$ as in VII.4.31 below. We also observe that if $a\sim a'$ and $b\sim b'$, then $a\preccurlyeq b$ yields $a'\preccurlyeq b'$ and $a\prec b$ yields $a'\prec b'$ (Exercise VII.39).

**VII.4.31 Alternative Definition (Cantor).** $\mathrm{Card}(a)<\mathrm{Card}(b)$ means $a\prec b$. $\mathrm{Card}(a)\leq\mathrm{Card}(b)$ means $a\preccurlyeq b$. □

The above definition embodies the equivalence of (i) and (iii) of Proposition VII.4.14. Here Theorem VII.4.9 trivially holds via VII.4.11(ii). "Cantor's theorem" (VII.4.16) also holds. The Cantor-Bernstein theorem is proved by the AC-free proof that follows VII.4.17 (p. 463). This yields that $<$ is a partial order on Cn. Indeed, irreflexivity is immediate ($\mathrm{Card}(a)<\mathrm{Card}(a)$ requires $a\not\sim a$). Transitivity is obtained as follows:

Let $\mathfrak{a}<\mathfrak{b}<\mathfrak{c}$ and therefore $\mathrm{Card}(a)<\mathrm{Card}(b)<\mathrm{Card}(c)$ for appropriate $a$, $b$ and $c$. By VII.4.31, $a\prec b\prec c$; hence $a\preccurlyeq c$ by Proposition VII.4.11(i). If $a\sim c$, then (Exercise VII.39) $b\prec a$, and hence $a\sim b$ by the Cantor-Bernstein theorem. Thus $a\prec c$, i.e., $\mathfrak{a}<\mathfrak{c}$.

Proposition VII.4.20 has the following counterpart:

**VII.4.32 Proposition.** *If $S$ is a nonempty set of cardinals, then there is a cardinal $\mathfrak{b}$ such that $\mathfrak{a} \le \mathfrak{b}$ for all $\mathfrak{a} \in S$.*

*Proof.* Let $T = \{\rho(\mathfrak{a}) : \mathfrak{a} \in S\}$. $T$ is a set (of ordinals) by collection; hence $\bigcup T$ is an ordinal $\alpha$ such that $\beta \le \alpha$ for all $\beta \in T$ (Theorem VI.5.22).

Thus $x \in \mathfrak{a} \in S$ implies $\rho(x) < \rho(\mathfrak{a}) \le \alpha$, so that

$$x \in V_N(\alpha) \tag{1}$$

By (1), $\mathfrak{a} \subseteq V_N(\alpha)$ for any $\mathfrak{a} \in S$. Thus $\mathfrak{b} = \text{Card}(V_N(\alpha))$ will do, by VII.4.11(ii). □

From the above, one obtains, once again, Corollary VII.4.21: If Cn is a set, then let $\mathfrak{b}$ satisfy $\mathfrak{a} \le \mathfrak{b}$ for all $\mathfrak{a} \in \text{Cn}$. Then since $\text{Card}(\mathbf{P}(\mathfrak{b})) \in \text{Cn}$, we get $\text{Card}(\mathbf{P}(\mathfrak{b})) \le \mathfrak{b}$, contradicting Cantor's theorem.

**VII.4.33 Exercise.** Comment on the alternative proof of Proposition VII.4.32 that proceeds as follows: Represent each $\mathfrak{a} \in S$ as $\text{Card}(a)$ for an appropriate set $a$. Let $T$ be the union of all these $a$'s. $T$ is a set and $a \subseteq T$ for each $a$. Thus $\mathfrak{a} = \text{Card}(a) \le \text{Card}(T)$ by VII.4.11(ii). Therefore, $\mathfrak{b} = \text{Card}(T)$ will do. □

The following is the counterpart of Theorem VII.4.26.

**VII.4.34 Theorem. (Hartogs (1915)).** *For any set $x$ there is an ordinal $\alpha$ such that $\alpha \not\preccurlyeq x$.*

*Proof.* Let $S = \{\beta : \beta \preccurlyeq x\}$. First, by VII.4.11(i), $S$ is transitive.

We next verify that $S$ is a set and therefore an ordinal, say $S = \alpha$. To see this, consider the class $W = \{\langle A, R\rangle : A \subseteq x \wedge R \subseteq A \times A \text{ is a well-ordering of } A\}$. Since $W \subseteq \mathbf{P}(x) \times \mathbf{P}(x \times x)$, $W$ is a set.

If $\langle A, R\rangle \in W$, then $\langle A, R\rangle \cong \beta$ for a unique $\beta$ via a unique order isomorphism $\phi_{A,R} : A \to \beta$. Clearly $\beta \in S$ by VII.4.11(iii), and conversely each $\beta \in S$ and any particular total 1-1 function $f : \beta \to x$ induces a well-ordering $R$ on $A = \text{ran}(f) \subseteq x$, so that $\beta = \|\langle A, R\rangle\|$ (VI.3.12 and VI.4.33).

We conclude that the function $\langle A, R\rangle \mapsto \|\langle A, R\rangle\| : W \to S$ is onto, and thus $S$ is a set by collection. If now $\alpha \preccurlyeq x$, then $\alpha \in \alpha$. We must conclude that $\alpha \not\preccurlyeq x$. □

We conclude this digression by observing that $<$ on cardinals, as these were defined in VII.4.27, is a partial order (see the discussion following Definition VII.4.31) but that without the axiom of choice it cannot be shown to be a total order. Of course, in the presence of AC one would rather define cardinals, as we do, by Definition VII.4.1.

**VII.4.35 Theorem. (Hartogs (1915)).** AC *is equivalent to the statement "$<$ of Definition VII.4.31 is a total order between cardinals, as these were defined in VII.4.27".*

*Proof.* First assume the statement in quotes and prove AC.

Let $x$ be any nonempty set and $\alpha$ be such that $\alpha \not\preccurlyeq x$ by Theorem VII.4.34. Thus neither $\text{Card}(\alpha) = \text{Card}(x)$ nor $\text{Card}(\alpha) < \text{Card}(x)$. By assumption $\text{Card}(x) < \text{Card}(\alpha)$, i.e., $x \prec \alpha$, say, via the total 1-1 function $f : x \rightarrow \alpha$.

$f^{-1} : \text{ran}(f) \rightarrow x$ well-orders $x$ by VI.3.12. This proves that every nonempty set can be well-ordered, and hence proves AC.

Assume AC now. By Zermelo's theorem, if $x$ and $y$ are sets, then $x \sim \alpha$ and $y \sim \beta$ for some $\alpha$ and $\beta$. Without loss of generality, say $\alpha \leq \beta$. Then $\alpha \preccurlyeq \beta$. Now invoke Exercise VII.39. □

## VII.5. Arithmetic on Cardinals

In set theory and other branches of mathematics one often wants to compute the cardinality of a set $a$ which is formed in a particular way from given sets whose cardinalities we already know. Failing this, one is often content to at least compute an *approximation* of the cardinality of $a$, preferably erring on the high side. This section develops some tools to carry out such computations.

**VII.5.1 Definition.** For any cardinals $\mathfrak{a}$ and $\mathfrak{b}$, $\mathfrak{a} +_c \mathfrak{b}$ stands for $\text{Card}(\{0\} \times \mathfrak{a} \cup \{1\} \times \mathfrak{b})$, their *sum.* □

The sum operation is denoted by the cumbersome $+_c$ to avoid confusion with ordinal addition.

**VII.5.2 Proposition.** *If $A$ and $B$ are disjoint sets, then* $\text{Card}(A) +_c \text{Card}(B) = \text{Card}(A \cup B)$.

*Proof.* Let $\mathfrak{a} = \text{Card}(A)$ and $\mathfrak{b} = \text{Card}(B)$. Since $\mathfrak{a} \sim \{0\} \times \mathfrak{a}$ via $x \mapsto \langle 0, x\rangle$ and $\mathfrak{b} \sim \{1\} \times \mathfrak{b}$ via $x \mapsto \langle 1, x\rangle$, there are 1-1 correspondences $f : A \rightarrow \{0\} \times \mathfrak{a}$ and $g : B \rightarrow \{1\} \times \mathfrak{b}$. Since $A \cap B = \{0\} \times \mathfrak{a} \cap \{1\} \times \mathfrak{b} = \emptyset$, it follows that $f \cup g$ is a 1-1 correspondence and $A \cup B \sim \{0\} \times \mathfrak{a} \cup \{1\} \times \mathfrak{b}$; thus $\mathfrak{a} +_c \mathfrak{b} = \text{Card}(A \cup B)$. □

**VII.5.3 Corollary.** *For any sets $A$ and $B$,* $\mathrm{Card}(A \cup B) \le \mathrm{Card}(A) +_c \mathrm{Card}(B)$.

*Proof.* The function $f : \{0\} \times A \cup \{1\} \times B \to A \cup B$ given by $\langle i, x\rangle \mapsto x$ is onto. The claim now follows from VII.5.2 and VII.4.14(ii). □

**VII.5.4 Remark.** By VII.5.2, to compute $\mathfrak{a} +_c \mathfrak{b}$ it suffices to compute $\mathrm{Card}(A \cup B)$ for *any* disjoint $A$ and $B$ that have cardinalities $\mathfrak{a}$ and $\mathfrak{b}$ respectively. This observation proves to be very convenient in practice. □

**VII.5.5 Example.** We verify that $\omega +_c \omega = \omega$. Indeed, observe that $\omega \sim \mathbb{E}$ and $\omega \sim \mathbb{O}$, where $\mathbb{E}$ and $\mathbb{O}$ are the even and odd natural numbers respectively, and apply VII.5.2.

It is important to observe that $+_c$ (cardinal addition) is different than $+$ on ordinals ($\omega \ne \omega + \omega$). □

**VII.5.6 Example (Informal).** We verify that $\omega +_c \mathrm{Card}(\mathbb{R}) = \mathrm{Card}(\mathbb{R})$.[†] Indeed, $(0, 1) \cap \omega = \emptyset$ and $(0, 1) \sim \mathbb{R}$ (Exercise VII.34). Thus

$$\omega +_c \mathrm{Card}(\mathbb{R}) = \mathrm{Card}(\omega \cup (0, 1)) \le \mathrm{Card}(\mathbb{R}) \tag{1}$$

where the $=$ follows from VII.5.2 and the $\le$ from $\omega \cup (0, 1) \subseteq \mathbb{R}$. Similarly, $\mathrm{Card}(\mathbb{R}) \le \mathrm{Card}(\omega \cup (0, 1))$ by Exercise VII.34 and $(0, 1) \preccurlyeq \omega \cup (0, 1)$. This and (1) establish the claim. Alternatively, $\omega \cup (0, 1) \sim (0, 1)$ by VII.2.24. □

The basic properties of addition, worked out by Cantor, are captured by the following theorem.

**VII.5.7 Proposition (Cantor).** *For any cardinals the following hold:*

$(i)$ $\mathfrak{a} +_c 0 = \mathfrak{a}$
$(ii)$ $\mathfrak{a} +_c \mathfrak{b} = \mathfrak{b} +_c \mathfrak{a}$
$(iii)$ $(\mathfrak{a} +_c \mathfrak{b}) +_c \mathfrak{c} = \mathfrak{a} +_c (\mathfrak{b} +_c \mathfrak{c})$
$(iv)$ *If* $\mathfrak{a} \le \mathfrak{b}$*, then* $\mathfrak{a} +_c \mathfrak{c} \le \mathfrak{b} +_c \mathfrak{c}$
$(v)$ $\mathfrak{a} \le \mathfrak{b}$ *iff for some* $\mathfrak{c}$, $\mathfrak{b} = \mathfrak{a} +_c \mathfrak{c}$.

*Proof.* $(i)$–$(iii)$: by VII.5.4.

For $(iv)$, let $A, B, C$ be mutually disjoint sets such that $\mathfrak{a} = \mathrm{Card}(A)$, $\mathfrak{b} = \mathrm{Card}(B)$, $\mathfrak{c} = \mathrm{Card}(C)$. By VII.4.14, there is an onto $f : B \to A$. Then $f \cup i : B \cup C \to A \cup C$ is an onto function, where $i : C \to C$ is the identity.

[†] The cardinality of the set of real numbers is often denoted by $c$ in the literature ("$c$" stands for "continuum").

For $(v)$, let $\mathfrak{a} \le \mathfrak{b}$ and $A$, $B$ be as above; hence (VII.4.14) there is a total, 1-1 $f : A \to B$. Let $C = B - \mathrm{ran}(f)$ (this might be empty). Set $\mathfrak{c} = \mathrm{Card}(C)$. Now, $C \cap \mathrm{ran}(f) = \emptyset$, and $\mathrm{Card}(\mathrm{ran}(f)) = \mathfrak{a}$. Thus, $\mathfrak{a} +_c \mathfrak{c} = \mathrm{Card}(\mathrm{ran}(f) \cup C) = \mathfrak{b}$. This settles the only-if part. For the if part start with $A \cap C = \emptyset$ such that $\mathfrak{a} = \mathrm{Card}(A)$, $\mathfrak{c} = \mathrm{Card}(C)$, and set $B = A \cup C$, $\mathfrak{b} = \mathrm{Card}(B) = \mathfrak{a} +_c \mathfrak{c}$. Since $i : A \subseteq B$ (the inclusion map, given by $i(x) = x$ for all $x \in A$) is total and 1-1, we get $\mathfrak{a} \le \mathfrak{b}$ by VII.4.14. □

**VII.5.8 Proposition.** $+_c \restriction \omega^2 = + \restriction \omega^2$.

*Proof.* $m + n = m \cup \{m + k : k \in n\}$ by V.1.25 (or VI.10.4). The function $f : n \to \{m + k : k \in n\}$, given by $f(k) = m + k$, is a 1-1 correspondence (1-1-ness by VI.10.2). Thus,

$$\begin{aligned} m + n &= \mathrm{Card}(m + n) \qquad \text{since } m + n \in \omega \\ &= \mathrm{Card}(m) +_c \mathrm{Card}(\{m + k : k \in n\}) \\ &= m +_c n \end{aligned}$$

□

We next turn to the multiplication of cardinals. The definition is motivated from the intuitive observation that if $|A| = n$ and $|B| = m$, then $|A \times B| = m \cdot n$. The validity of this observation will be formally verified below.

**VII.5.9 Definition.** For any cardinals $\mathfrak{a}$ and $\mathfrak{b}$, $\mathfrak{a} \cdot_c \mathfrak{b}$ stands for $\mathrm{Card}(\mathfrak{a} \times \mathfrak{b})$, their *product*. □

The cumbersome "$\cdot_c$" for cardinal multiplication is used to distinguish this operation from "$\cdot$", ordinal multiplication. We prove the analogue of VII.5.2 first:

**VII.5.10 Proposition.** *If* $\mathfrak{a} = A$ *and* $\mathfrak{b} = B$, *then* $\mathfrak{a} \cdot_c \mathfrak{b} = \mathrm{Card}(A \times B)$.

*Proof.* Let $f : \mathfrak{a} \to A$ and $g : \mathfrak{b} \to B$ be 1-1 correspondences. It follows that $\lambda\gamma\delta.\langle f(\gamma), g(\delta)\rangle$ is a 1-1 correspondence $\mathfrak{a} \times \mathfrak{b} \to A \times B$. □

**VII.5.11 Example.** In view of VII.2.9, $\omega \cdot_c \omega = \omega < \omega \cdot \omega$; thus

$$\mathfrak{a} \cdot_c \mathfrak{b} \ne \mathfrak{a} \cdot \mathfrak{b}, \qquad \textit{in general.}$$

See however below, the case of *finite* cardinals. □

**VII.5.12 Proposition.** $\cdot_c \restriction \omega^2 = \cdot \restriction \omega^2$.

*Proof.* We have

$$\begin{aligned} m \cdot n &= \mathrm{Card}(m \cdot n) && \text{since } m \cdot n \in \omega \\ &= \mathrm{Card}(n \times m) && \text{by VI.10.18} \\ &= \mathrm{Card}(m \times n) && \text{via } \langle k, l\rangle \mapsto \langle l, k\rangle \\ &= m \cdot_c n && \text{by VII.5.9} \end{aligned}$$

□

**VII.5.13 Proposition (Cantor).** *For any cardinals, the following hold:*

$(i)$ $\mathfrak{a} \cdot_c 0 = 0$

$(ii)$ $\mathfrak{a} \cdot_c 1 = \mathfrak{a}$

$(iii)$ $\mathfrak{a} \cdot_c \mathfrak{b} = \mathfrak{b} \cdot_c \mathfrak{a}$

$(iv)$ $(\mathfrak{a} \cdot_c \mathfrak{b}) \cdot_c \mathfrak{c} = \mathfrak{a} \cdot_c (\mathfrak{b} \cdot_c \mathfrak{c})$

$(v)$ *If* $\mathfrak{a} \le \mathfrak{b}$, *then* $\mathfrak{a} \cdot_c \mathfrak{c} \le \mathfrak{b} \cdot_c \mathfrak{c}$

$(vi)$ $\mathfrak{a} \cdot (\mathfrak{b} +_c \mathfrak{c}) = \mathfrak{a} \cdot_c \mathfrak{b} + \mathfrak{a} \cdot_c \mathfrak{c}$.

*Proof.* We apply VII.5.10 throughout. Thus, $(i)$ follows from $A \times \emptyset = \emptyset$. $(ii)$ follows from the fact that $x \mapsto \langle x, 0\rangle$ is a 1-1 correspondence $A \to A \times 1$. For $(iii)$ note that $A \times B \sim B \times A$ via $\langle x, y\rangle \mapsto \langle y, x\rangle$. $(iv)$ is a consequence of $(A \times B) \times C \sim A \times (B \times C)$ via $\langle x, y, z\rangle \mapsto \langle x, \langle y, z\rangle\rangle$ (recall that $\langle x, y, z\rangle = \langle\langle x, y\rangle, z\rangle$).

For $(v)$, let $f : A \to B$ be 1-1 and total. Then $\langle x, y\rangle \mapsto \langle f(x), y\rangle$ is 1-1 and total $A \times C \to B \times C$.

Finally, for $(vi)$, take $\mathfrak{b} = \mathrm{Card}(B)$ and $\mathfrak{c} = \mathrm{Card}(C)$ with $B \cap C = \emptyset$, and note that $A \times (B \cup C) = (A \times B) \cup (A \times C)$ and that $(A \times B) \cap (A \times C) = \emptyset$.

□

The following result, along with the Cantor-Bernstein theorem, assists in computations where $+_c$ and $\cdot_c$ are involved. It shows that cardinal addition and multiplication are nowhere near as rich as their ordinal counterparts.

**VII.5.14 Theorem.** *For any* $\mathfrak{a} \ge \omega$, $\mathfrak{a} \cdot_c \mathfrak{a} = \mathfrak{a}$.

*Proof.* Let $\mathfrak{a} \ge \omega$ be the smallest cardinal for which the claim fails. Then $\mathfrak{a} > \omega$ by VII.5.11. Let $\mathfrak{a} \times \mathfrak{a} \cong \beta$, via the $J$ of Section VI.7, i.e., $J[\mathfrak{a} \times \mathfrak{a}] = \beta$. We know that $J[\mathfrak{a} \times \mathfrak{a}] \ge \mathfrak{a}$ by Exercise VI.30, so $\mathfrak{a} < \beta$; therefore

$$\mathfrak{a} \cong \lhd\big(\langle \gamma, \delta\rangle\big) \qquad \text{for some } \langle \gamma, \delta\rangle \in \mathfrak{a} \times \mathfrak{a} \tag{1}$$

Since $\mathrm{Lim}(\mathfrak{a})$ (by VII.4.8), take a $\lambda < \mathfrak{a}$ to satisfy also $\max(\gamma, \delta) < \lambda$. Thus, the isomorphism in (1) establishes $\mathfrak{a} \preccurlyeq \lambda \times \lambda$. Therefore

$$\mathfrak{a} = \mathrm{Card}(\mathfrak{a}) \leq \mathrm{Card}(\lambda \times \lambda) = \mathrm{Card}(\lambda) \cdot_c \mathrm{Card}(\lambda) = \mathrm{Card}(\lambda) \qquad (2)$$

the last "=" by minimality of $\mathfrak{a}$, and $\mathrm{Card}(\lambda) \leq \lambda < \mathfrak{a}$ (using VII.4.6). We now have a contradiction $\mathfrak{a} \leq \mathrm{Card}(\lambda) < \mathfrak{a}$. □

A side effect of the proof is that $J[\aleph_\alpha \times \aleph_\alpha] \cong \aleph_\alpha$ for all $\alpha$.

**VII.5.15 Corollary.** *For any* $\mathfrak{a} \geq \omega$, $\mathfrak{a} +_c \mathfrak{a} = \mathfrak{a}$.

*Proof.* Using the arithmetic of VII.5.13,

$$\begin{aligned}
\mathfrak{a} +_c \mathfrak{a} &= \mathfrak{a} \cdot_c 1 +_c \mathfrak{a} \cdot_c 1 \\
&= \mathfrak{a} \cdot_c (1 +_c 1) \\
&= \mathfrak{a} \cdot_c (1 + 1) \\
&= \mathfrak{a} \cdot_c 2 \\
&\leq \mathfrak{a} \cdot_c \mathfrak{a} \qquad \text{by VII.5.13}(iii) \text{ and } (v) \\
&= \mathfrak{a}
\end{aligned}$$

But we also have $\mathfrak{a} \leq \mathfrak{a} +_c \mathfrak{a}$. □

**VII.5.16 Example.** Constructions in mathematics often result in a family of sets $(A_i)_{i \in I}$ where we have the "estimates" of cardinalities

$$\mathrm{Card}(A_i) \leq \mathfrak{a} \qquad \text{for all } i \in I \qquad (1)$$

and

$$\mathrm{Card}(I) \leq \mathfrak{b} \qquad (2)$$

We can then estimate that

$$\mathrm{Card}\left(\bigcup_{i \in I} A_i\right) \leq \mathfrak{a} \cdot_c \mathfrak{b} \qquad (3)$$

Indeed, using AC, pick for each $i \in I$ an onto $f_i : \mathfrak{a} \to A_i$, which is legitimate by (1). Define $g : \mathfrak{a} \times I \to \bigcup_{i \in I} A_i$ by

$$g(\gamma, i) = f_i(\gamma) \qquad \text{for all } \gamma \in \mathfrak{a},\ i \in I$$

Now $g$ is onto; hence

$$\mathrm{Card}\left(\bigcup_{i \in I} A_i\right) \leq \mathrm{Card}(\mathfrak{a} \times I) = \mathfrak{a} \cdot_c \mathrm{Card}(I) \leq \mathfrak{a} \cdot_c \mathfrak{b}$$

That is (3). □

Apart from our use of AC in the definition of cardinals (through the well-ordering theorem), the above result also invoked AC (twice) additionally (why twice?). AC can be avoided if we are content to prove instead: “Assume that cardinals were defined without AC, say as in VII.4.27. Now, assume (1) and (2) above, and moreover let $I$ and $\bigcup_{i \in I} A_i$ be well-orderable. Then (3) follows within ZF.”

Indeed, let $\alpha = \|(\bigcup_{i \in I} A_i, <_1)\|$ with respect to some arbitrarily chosen well-ordering $<_1$ of this set. Let us also pick a well-ordering $<_2$ of $I$. Define for each $x \in \bigcup_{i \in I} A_i$

$$f(x) = \langle i, \gamma \rangle, \qquad \begin{aligned} &\text{where } i = (<_2\text{-min})\{j \in I : x \in A_j\} \text{ and} \\ &\gamma = \|(<_1 \langle x \rangle, <_1)\| \end{aligned}$$

Clearly, $f : \bigcup_{i \in I} A_i \to I \times \alpha$ is total and 1-1. Hence,

$$\operatorname{Card}\left(\bigcup_{i \in I} A_i\right) \leq \operatorname{Card}(I \times \alpha) = \operatorname{Card}(I) \cdot_c \operatorname{Card}(\alpha) = \mathfrak{b} \cdot_c \mathfrak{a} = \mathfrak{a} \cdot_c \mathfrak{b}$$

**VII.5.17 Example.** Here is a situation where we may want to use the technique of the previous example: We have a first order language of logic, where the set of *nonlogical* symbols has cardinality $\mathfrak{k}$. How “many” formulas can this language have? Well, no more than *strings* over the alphabet of the language. Now the cardinality of the alphabet, $L$, is

$$\operatorname{Card}(L) = \omega +_c \mathfrak{k} = \begin{cases} \omega & \text{if } \mathfrak{k} \leq \omega \\ \mathfrak{k} & \text{otherwise} \end{cases}$$

where $\omega$ is the cardinality of the set of *logical* symbols (assuming the object variables are $v_0, v_1, \ldots$).

A “string” of length $n < \omega$ is, of course, a member of $L^n$. An easy induction on $n$, via VII.5.14, shows that

$$\operatorname{Card}(L^n) = \begin{cases} \omega & \text{if } \mathfrak{k} \leq \omega \\ \mathfrak{k} & \text{otherwise} \end{cases}$$

Thus, the set of all strings over $L$, $\bigcup_{n \in \omega} L^n$, has cardinality

$$\operatorname{Card}\left(\bigcup_{n \in \omega} L^n\right) \leq \begin{cases} \omega \cdot_c \omega = \omega & \text{if } \mathfrak{k} \leq \omega \\ \mathfrak{k} \cdot_c \omega = \mathfrak{k} & \text{otherwise} \end{cases}$$

Can you sharpen the $\leq$ into $=$? □

We define, finally, cardinal exponentiation. This again turns out to be far too “easy” by comparison with ordinal exponentiation.

**VII.5.18 Definition.** For any $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{a}^{\mathfrak{b}}$ denotes $\mathrm{Card}({}^{\mathfrak{b}}\mathfrak{a})$. □

First, let us give the analogues of VII.5.2 and VII.5.10.

**VII.5.19 Proposition.** *If* $\mathfrak{a} = \mathrm{Card}(A)$ *and* $\mathfrak{b} = \mathrm{Card}(B)$*, then* $\mathrm{Card}({}^{\mathfrak{b}}\mathfrak{a}) = \mathrm{Card}({}^{B}A)$.

*Proof.* Let $f : \mathfrak{a} \to A$ and $g : \mathfrak{b} \to B$ be 1-1 correspondences. As the following commutative diagram (cf. V.3.11) shows, $F : {}^{\mathfrak{b}}\mathfrak{a} \to {}^{B}A$ given by

$$F(h) = f \circ h \circ g^{-1}$$

is a 1-1 correspondence, with inverse $\lambda k.f^{-1} \circ k \circ g : {}^{B}A \to {}^{\mathfrak{b}}\mathfrak{a}$:

$$\begin{tikzcd}
\mathfrak{b} \arrow[r, "h", "F^{-1}(k)"'] & \mathfrak{a} \arrow[d, "f"] \\
B \arrow[u, "g^{-1}"] \arrow[r, "k", "F(h)"'] & A
\end{tikzcd}$$

□

**VII.5.20 Remark.** By VII.3.9, $2^{\mathrm{Card}(A)} = \mathrm{Card}({}^{A}2) = \mathrm{Card}(\mathbf{P}(A))$ for all sets $A$.

In particular,

$$\begin{aligned} 2^{\aleph_0} &= \mathrm{Card}(\mathbf{P}(\omega)) \\ &= c, \quad \text{by VII.3.8} \end{aligned}$$

□

**VII.5.21 Proposition (Cantor).** *Cardinal exponentiation obeys the following:*

$(i)$ $\mathfrak{a}^0 = 1$
$(ii)$ $\mathfrak{a}^1 = \mathfrak{a}$
$(iii)$ $\mathfrak{a}^{\mathfrak{k} +_c \mathfrak{l}} = \mathfrak{a}^{\mathfrak{k}} \cdot_c \mathfrak{a}^{\mathfrak{l}}$
$(iv)$ $(\mathfrak{a}^{\mathfrak{k}})^{\mathfrak{l}} = \mathfrak{a}^{(\mathfrak{k} \cdot_c \mathfrak{l})}$
$(v)$ $\mathfrak{a}^{\mathfrak{k}} \le \mathfrak{b}^{\mathfrak{k}}$ *whenever* $\mathfrak{a} \le \mathfrak{b}$.

*Proof.* $(i)$: The empty function 0 is the only member of ${}^{0}\mathfrak{a}$; hence $\mathrm{Card}({}^{0}\mathfrak{a}) = 1$. For $(ii)$, the set of total functions $f : 1 \to \mathfrak{a}$ is ${}^{1}\mathfrak{a} = \{\{\langle 0, \gamma\rangle\} : \gamma < \mathfrak{a}\}$. Thus $\mathrm{Card}({}^{1}\mathfrak{a}) = \mathfrak{a}$, via the 1-1 correspondence $\{\langle 0, \gamma\rangle\} \mapsto \gamma$.

$(iii)$: Let $\mathfrak{k} = \mathrm{Card}(K)$, $\mathfrak{l} = \mathrm{Card}(L)$, $\mathfrak{a} = \mathrm{Card}(A)$, where $K \cap L = \emptyset$. The reader can readily verify that $f \mapsto \langle f \restriction K, f \restriction L\rangle$ is a 1-1 correspondence ${}^{K\cup L}A \sim {}^{K}A \times {}^{L}A$.

$(iv)$: Let $K, L, A$ be as in $(iii)$ (although $K \cap L = \emptyset$ is not required here). We need a 1-1 correspondence ${}^{(K\times L)}A \sim {}^{L}({}^{K}A)$. The function that maps $\lambda xy.f(x, y) \in {}^{(K\times L)}A$ to $\lambda y.(\lambda x.f(x, y)) \in {}^{L}({}^{K}A)$ fills the bill.

$(v)$: Since $\mathfrak{a} \subseteq \mathfrak{b}$, $F : {}^{\mathfrak{k}}\mathfrak{a} \to {}^{\mathfrak{k}}\mathfrak{b}$ given by $F(g) = g$ is total and 1-1. □

The next result shows that cardinal exponentiation coincides with ordinal exponentiation over $\omega$, just like the addition and multiplication.

**VII.5.22 Proposition.** *For all $m, n$ in $\omega$, $m^{\cdot n} = m^n$.*

*Proof.* Induction on $n$. For $n = 0$ we have $m^{\cdot 0} = 1 = m^0$, the last equality by VII.5.21. Assume the claim for some frozen $n$, and proceed to $n + 1$.

$$\begin{aligned} m^{\cdot(n+1)} &= m^{\cdot n} \cdot m && \text{by VI.10.23}\\ &= m^n \cdot_c m && \text{by I.H. and VII.5.12}\\ &= m^n \cdot_c m^1 && \text{by VII.5.21}\\ &= m^{n+_c 1} && \text{by VII.5.21}\\ &= m^{n+1}, && \text{by VII.5.8} \end{aligned}$$

□

**VII.5.23 Example.** How big is $\aleph_0^{\aleph_0}$? Well, this is $\mathrm{Card}({}^{\omega}\omega)$; therefore

$$\begin{aligned} c &= \mathrm{Card}({}^{\omega}2)\\ &\le \mathrm{Card}({}^{\omega}\omega) && \text{since } {}^{\omega}2 \subseteq {}^{\omega}\omega\\ &\le \mathrm{Card}\big(\mathbf{P}(\omega\times\omega)\big) && \text{since } {}^{\omega}\omega \subseteq \mathbf{P}(\omega\times\omega)\\ &= \mathrm{Card}({}^{\omega\times\omega}2) && \text{by VII.3.9}\\ &= c && \text{by VII.5.20 and VII.2.9} \end{aligned}$$

Thus, $\aleph_0^{\aleph_0} = c$. □

**VII.5.24 Example.** For any $n \in \omega - \{0\}$ and set $A$, we have $A^n \sim {}^{n}A$ via the 1-1 correspondence $\langle x_0, \ldots x_{n-1}\rangle \mapsto \{\langle i, x_i\rangle : i \in n\}$. Thus $\mathrm{Card}({}^{n}A) = \mathrm{Card}(A^n)$.

In particular, $\mathfrak{a}^2 = \mathrm{Card}({}^{2}\mathfrak{a}) = \mathrm{Card}(\mathfrak{a}\times\mathfrak{a}) = \mathfrak{a}\cdot_c\mathfrak{a}$ for any $\mathfrak{a}$. □

**VII.5.25 Remark.** We saw in the discussion following VII.4.26 (p. 466) that

$$(\aleph_\alpha)^+ \le \mathrm{Card}(\mathbf{P}(\aleph_\alpha))$$

or

$$(\aleph_\alpha)^+ \le \mathrm{Card}({}^{\aleph_\alpha}2) = 2^{\aleph_\alpha}$$

Thus,

(1) an alternative formulation of GCH is

$$\aleph_{\alpha+1} = 2^{\aleph_\alpha}$$

and

(2) we have just estimated $\mathfrak{a}^+$ in general:

$$\mathfrak{a}^+ \le 2^{\mathfrak{a}}$$

□ ☡

## VII.6. Cofinality; More Cardinal Arithmetic; Inaccessible Cardinals

How far can we "stretch" an ordinal $\alpha$ by applying to it a function $f$? That is, given $\alpha$ and a total function $f : \alpha \to \mathrm{On}$, how "big" can the elements of $\mathrm{ran}(f)$ be? Well, let $\beta$ be arbitrary. Define $f(0) = \beta$. Thus $1 = \{0\}$ is stretched, by $f$, to the arbitrarily large value $\beta$. Clearly an uninspiring answer.

A much better question to ask, which leads to fruitful answers, is: how far can we *shrink* a given ordinal $\alpha$ by some total function, $f$? That is, what is the *smallest* $\beta$ such that $f : \beta \to \alpha$ and $\mathrm{ran}(f)$ "spreads as far to the right" in $\alpha$ as possible?

More precisely, let us define

**VII.6.1 Definition (Cofinal Subsets).** Let $\emptyset \ne A \subseteq B$, and $<$ be an order on $B$ (hence also on $A$). We say that $A$ is *cofinal in $B$* just in case for every $b \in B$ there is an $a \in A$ such that $b \le a$, where, of course, $x \le y$ means $x < y \lor x = y$. □

The set $A$ above "spreads as far to the right in $B$ as possible". If $\beta \subseteq \alpha$, then $\beta$ cannot be cofinal in $\alpha$ in the above sense, unless $\beta = \alpha$. For this reason we have a somewhat different notion of "cofinal in" for ordinals.

**VII.6.2 Definition.** $\beta$ is *cofinal* in $\alpha \ne 0$ just in case there is a *total* function $f : \beta \to \alpha$ such that $\mathrm{ran}(f)$ is cofinal in $\alpha$ *in the sense of* VII.6.1. We say that $f$ maps $\beta$ *cofinally* into $\alpha$, and that $f : \beta \to \alpha$ is a cofinal map (function).

The *cofinality* of an ordinal $\alpha$, $\mathrm{cf}(\alpha)$, is the smallest ordinal that is cofinal in $\alpha$. □

Thus, $\mathrm{cf}(\alpha)$ is the smallest ordinal into which we can "shrink" $\alpha$ via a (total) function. If $\mathrm{Lim}(\alpha)$, and $f : \beta \to \alpha$ is cofinal, then $\mathrm{ran}(f)$ is *unbounded in* $\alpha$ (hence $\sup \mathrm{ran}(f) = \bigcup \mathrm{ran}(f) = \alpha$), since $\gamma < \alpha$ implies $\gamma + 1 < \alpha$, and hence $\gamma < \gamma + 1 \le f(\sigma)$ for some $\sigma \in \beta$.[†]

From the preamble to the section it follows that $1 = \mathrm{cf}(\alpha + 1)$ for any $\alpha$. Also, $\omega = \mathrm{cf}(\omega)$, since for each $n \in \omega$ and $f : n \to \omega$, $\mathrm{ran}(f)$ is finite (Exercise VII.18); hence $\bigcup \mathrm{ran}(f) \in \omega$, and thus, for all $n \in \omega$, $\mathrm{cf}(\omega) \ne n$. Also, by VII.4.23, $\mathrm{cf}(\aleph_\omega) = \omega$; therefore some "huge" ordinals (in this case a cardinal) can shrink quite a bit.

Finally, it is clear that $\mathrm{cf}(\alpha) \le \alpha$, since, whenever $\mathrm{Lim}(\alpha)$, the identity function maps $\alpha$ cofinally into $\alpha$, while when $\alpha = \beta + 1$, $\mathrm{cf}(\alpha) = 1 \le \alpha$.

**VII.6.3 Definition (Hausdorff).** An ordinal $\alpha$ is *regular* provided $\mathrm{cf}(\alpha) = \alpha$. Otherwise, it is *singular*. □

Thus, 1 and $\omega$ are regular, all $n > 1$ in $\omega$ are singular, and so is $\aleph_\omega$.[‡]

**VII.6.4 Proposition.** *For any* $\alpha$, $\mathrm{cf}(\alpha)$ *is a cardinal.*

*Proof.* If $\alpha$ is a successor then the result is trivial. Otherwise, let $1 \le \beta < \mathrm{cf}(\alpha)$ and $g : \beta \to \mathrm{cf}(\alpha)$ be a 1-1 correspondence. Suppose that $f$ maps $\mathrm{cf}(\alpha)$ to $\alpha$ cofinally. Thus, $\bigcup \mathrm{ran}(f) = \alpha$. Clearly $\bigcup \mathrm{ran}(f \circ g) = \alpha$ as well, thus $f \circ g$ maps $\beta$ cofinally into $\alpha$, contradicting the minimality of $\mathrm{cf}(\alpha)$. □

Thus, all regular ordinals are cardinals. In particular, all, except 1, are limit ordinals.

**VII.6.5 Proposition.** *There is a total order-preserving cofinal map* $f : \mathrm{cf}(\alpha) \to \alpha$.

*Proof.* The result is trivial if $\alpha$ is a successor.

Let then $\mathrm{Lim}(\alpha)$, and $g : \mathrm{cf}(\alpha) \to \alpha$ be such that $\bigcup \mathrm{ran}(g) = \alpha$. Define $f$ by recursion for all $\beta \in \mathrm{cf}(\alpha)$

$$f(\beta) \simeq g(\min\{\sigma \in \mathrm{cf}(\alpha) : (\forall \gamma < \beta) g(\sigma) > f(\gamma) \cup g(\beta)\}) \tag{1}$$

[†] Some authors offer the definition only for $\mathrm{Lim}(\alpha)$.

[‡] If we allowed nontotal cofinal maps, then the modified definition would make 0 regular as well (Hausdorff). There is no universal agreement in the literature (see also previous footnote) on this point.

To see that $f$ is total on $\mathrm{cf}(\alpha)$, we argue that, for $\beta \in \mathrm{cf}(\alpha)$,

$$\{\sigma \in \mathrm{cf}(\alpha) : (\forall\gamma < \beta) g(\sigma) > f(\gamma) \cup g(\beta)\} \neq \emptyset \tag{2}$$

By (1), $\mathrm{ran}(f) \subseteq \alpha$. Thus, (2) follows, since

(i) $\mathrm{ran}(g)$ is unbounded in $\alpha$,
(ii) $\sup \mathrm{ran}(f \restriction \beta) < \alpha$, since $\beta < \mathrm{cf}(\alpha)$.

Again by (1), $f(\gamma) < f(\beta)$ if $\gamma < \beta$, so that $f$ is order-preserving.

Finally, $\tau \in \alpha$ implies $\tau < g(\sigma)$ for some $\sigma \in \mathrm{cf}(\alpha)$ by (i). By (1), $g(\sigma) < f(\sigma)$; hence $\tau \in \bigcup \mathrm{ran}(f)$; therefore $\alpha \subseteq \bigcup \mathrm{ran}(f)$; thus $\alpha = \bigcup \mathrm{ran}(f)$. □

**VII.6.6 Proposition.** *Let the order-preserving function $f$ map $\alpha$ cofinally into $\beta > \alpha$. Then* $\mathrm{cf}(\alpha) = \mathrm{cf}(\beta)$.

*Proof.* Let $g : \mathrm{cf}(\alpha) \to \alpha$ be a cofinal map. Then, so is $f \circ g : \mathrm{cf}(\alpha) \to \beta$. Indeed, let $\gamma \in \beta$. By cofinality of $f$, $f(\sigma) \geq \gamma$ for some $\sigma \in \alpha$. Moreover (cofinality of $g$) $g(\xi) \geq \sigma$ (for some $\xi \in \mathrm{cf}(\alpha)$). Since $f$ is order-preserving, $f(g(\xi)) \geq f(\sigma) \geq \gamma$. We conclude that

$$\mathrm{cf}(\beta) \leq \mathrm{cf}(\alpha) \tag{1}$$

If $\alpha$ is a successor, then $\mathrm{cf}(\alpha) = 1$ and the result follows from (1).

So let $\mathrm{Lim}(\alpha)$, and let $h : \mathrm{cf}(\beta) \to \beta$ be cofinal. Define a function $F : \beta \to \alpha$ by

$$F(\gamma) = \begin{cases} f^{-1}(\gamma) & \text{if } \gamma \in \mathrm{ran}(f) \\ \min\{\delta \in \alpha : f(\delta) > \gamma\} & \text{if } \gamma \notin \mathrm{ran}(f) \end{cases} \quad \text{for all } \gamma \in \beta$$

$F$ is total, for the min in the bottom case always exists. Indeed, given $\gamma$, there is a $\sigma \in \alpha$ such that $\gamma \leq f(\sigma) < f(\sigma + 1)$ [$\sigma + 1 \in \alpha$ by $\mathrm{Lim}(\alpha)$]. Hence $(\exists\delta \in \alpha) f(\delta) > \gamma$. Moreover,

$$F(\gamma) < F(\delta) \qquad \text{whenever } \mathrm{ran}(f) \ni \gamma < \delta \in \beta \tag{2}$$

Indeed, (2) is immediate if $\delta \in \mathrm{ran}(f)$ as well, since $f$ is order-preserving. If, on the other hand, $\delta \notin \mathrm{ran}(f)$, then let $\sigma \in \alpha$ be minimum such that $f(\sigma) > \delta$. Thus, $f(\sigma) > \delta > \gamma = f(\eta)$ for some $\eta \in \alpha$, and $F(\delta) = \sigma > \eta = F(\gamma)$.

Finally, $F \circ h : \mathrm{cf}(\beta) \to \alpha$ is cofinal. Indeed, let $\gamma \in \alpha$ and $\alpha \ni \delta > \gamma$ (by $\mathrm{Lim}(\alpha)$). Therefore $f(\delta) > f(\gamma)$. By cofinality of $h$, take $h(\sigma) > f(\delta)$, for some $\sigma \in \mathrm{cf}(\beta)$ (strict inequality by $\mathrm{Lim}(\beta)$ – why $\mathrm{Lim}(\beta)$?). It follows, using (2), that $F(h(\sigma)) > F(f(\delta)) = \delta > \gamma$.

Thus $\mathrm{cf}(\alpha) \leq \mathrm{cf}(\beta)$, and we are done by (1). □

**VII.6.7 Corollary.** *For any $\alpha$,* $\mathrm{cf}(\mathrm{cf}(\alpha)) = \mathrm{cf}(\alpha)$.

*Proof.* If $\alpha$ is regular, then the result is trivial. Otherwise, use VII.6.5 and VII.6.6. □

Thus, for all $\alpha$, $\mathrm{cf}(\alpha)$ is a regular cardinal.

**VII.6.8 Corollary.** *If $F$ is normal, then* $\mathrm{cf}(F(\alpha)) = \mathrm{cf}(\alpha)$ *for all limit ordinals $\alpha$.*

*Proof.* Since $F$ is order-preserving, $F(\alpha) \geq \alpha$. If we have equality, the result is trivial. So let $F(\alpha) > \alpha$. The map

$$\alpha \ni \beta \mapsto F(\beta) \in F(\alpha)$$

is cofinal by normality. The result then follows from VII.6.6. □

**VII.6.9 Corollary.** *For all* $\mathrm{Lim}(\alpha)$*,* $\mathrm{cf}(\aleph_\alpha) = \mathrm{cf}(\alpha)$.

*Proof.* $\alpha \mapsto \aleph_\alpha$ is normal. □

One often encounters, and accepts as common sense, the following statement: "Let $X \subseteq \bigcup_{n\in\omega} A_n$ and $X$ be finite. Then, for some $m \in \omega$, $X \subseteq \bigcup_{n<m} A_n$." This is a special case of the following.

**VII.6.10 Proposition.** *If* $\mathfrak{m} \geq \omega$ *is* regular, $\mathrm{Card}(X) < \mathfrak{m}$, *and* $X \subseteq \bigcup_{\lambda<\mathfrak{m}} A_\lambda$, *then* $X \subseteq \bigcup_{\lambda<\kappa} A_\lambda$ *for some* $\kappa < \mathfrak{m}$.

*Proof.* Let $\mathrm{Card}(X) = \mathfrak{n} < \mathfrak{m}$, and $g : \mathfrak{n} \to X$ be a 1-1 correspondence. Define $f : \mathfrak{n} \to \mathfrak{m}$ by

$$f(\sigma) = \min\left\{\tau \in \mathfrak{m} : g(\sigma) \notin \bigcup_{\lambda<\tau} A_\lambda\right\}$$

If the conclusion is false, then $f$ maps $\mathfrak{n}$ cofinally into $\mathfrak{m}$, contradicting the regularity of the latter. □

**VII.6.11 Proposition.** *The infinite cardinal $\mathfrak{a}$ is singular iff, for some $\beta < \mathfrak{a}$ and a family of sets $(A_\alpha)_{\alpha<\beta}$ with* $\mathrm{Card}(A_\alpha) < \mathfrak{a}$ *for all sets in the family, one has* $\mathfrak{a} = \mathrm{Card}(\bigcup_{\alpha<\beta} A_\alpha)$.

*Proof. Only-if part.* Let $\beta = \mathrm{cf}(\mathfrak{a}) < \mathfrak{a}$, and $f : \beta \to \mathfrak{a}$ be cofinal. Thus $\mathfrak{a} = \bigcup_{\alpha<\beta} f(\alpha)$. The result follows using $A_\alpha = f(\alpha)$. Of course, $f(\alpha) < \mathfrak{a}$; hence $\mathrm{Card}(f(\alpha)) \le f(\alpha) < \mathfrak{a}$.

*If part.* Suppose that $\mathfrak{a} = \mathrm{Card}(\bigcup_{\alpha<\beta} A_\alpha)$, where $\beta$ is the smallest ordinal that satisfies the hypotheses above. For each $\alpha \in \beta$ set $f(\alpha) = \mathrm{Card}(\bigcup_{\gamma<\alpha} A_\gamma)$. As $\bigcup_{\gamma<\alpha} A_\gamma \subseteq \bigcup_{\alpha<\beta} A_\alpha$, it follows that $\mathrm{Card}(\bigcup_{\gamma<\alpha} A_\gamma) \le \mathrm{Card}(\bigcup_{\alpha<\beta} A_\alpha) = \mathfrak{a}$. The $\le$ graduates to $<$ by minimality of $\beta$; hence $f(\alpha) \in \mathfrak{a}$ ($\in$ is, of course, $<$). Thus we have a function $f : \beta \to \mathfrak{a}$.

By VII.4.20, $\mathfrak{c} = \bigcup_{\alpha<\beta} f(\alpha) = \sup_{\alpha<\beta} f(\alpha)$ is a cardinal. Clearly, $\mathfrak{c} \le \mathfrak{a}$. Can the inequality be strict? Well, if it can, then (using VII.5.16)

$$\begin{aligned}
\mathfrak{a} &= \mathrm{Card}\left(\bigcup_{\alpha<\beta} A_\alpha\right)\\
&= \mathrm{Card}\left(\bigcup_{\alpha<\beta}\bigcup_{\gamma<\alpha} A_\gamma\right)\\
&\le \mathfrak{c} \cdot_c \mathrm{Card}(\beta) = \max\{\mathfrak{c}, \mathrm{Card}(\beta)\} < \mathfrak{a}
\end{aligned}$$

– a contradiction. Thus, $\mathfrak{c} = \mathfrak{a}$ and $f$ is cofinal. Since $\beta < \mathfrak{a}$, the result follows. □

(1) The above proposition can be rephrased to read exactly as above, but with $\beta$ replaced by a *cardinal* $\mathfrak{b} < \mathfrak{a}$. In the only-if part this is so because $\mathrm{cf}(\mathfrak{a})$ is a cardinal. In the if part it is so because the smallest ordinal $\beta$ that makes the proof work is $\mathrm{cf}(\mathfrak{a})$. But this is a cardinal.

(2) As the notions “singular” and “regular” pertain to ordinals, the remark following VII.5.16 applies here, so that VII.6.11 is provable within ZF on the assumption $\mathfrak{a}$ is well-orderable. Remarks such as that and the present one are only of value when one wants to gauge with accuracy which results follow, or do not follow, from what axioms.

**VII.6.12 Proposition.** *Every infinite successor cardinal is regular.*

*Proof.* Let $\omega \le \mathfrak{a}$, and assume instead that $\kappa = \mathrm{cf}(\mathfrak{a}^+) < \mathfrak{a}^+$ ($\kappa$ is a cardinal by VII.6.4). Let $f : \kappa \to \mathfrak{a}^+$ be cofinal. We observe that $f(\beta) < \mathfrak{a}^+$, hence $\mathrm{Card}(f(\beta)) \le \mathfrak{a}$, for all $\beta \in \kappa$. Thus, using VII.5.16,

$$\begin{aligned}
\mathfrak{a}^+ &= \bigcup_{\beta<\kappa} f(\beta)\\
&\le \kappa \cdot_c \mathfrak{a}\\
&\le \mathfrak{a} \cdot_c \mathfrak{a} = \mathfrak{a}
\end{aligned}$$

which is a contradiction. □

It is known that without AC we cannot prove (in ZF) that $\aleph_1$ is regular (Feferman and Levy (1963)). One cannot even prove (in ZF) that there are any infinite regular cardinals at all beyond $\omega$ (Gitik (1980)).

Let us next turn our attention to regular limit cardinals beyond $\omega$. These have a special name.

**VII.6.13 Definition.** A cardinal $\mathfrak{a} > \aleph_0$ is *weakly inaccessible* iff it is regular and a limit (i.e., for some $\alpha$ with $\mathrm{Lim}(\alpha)$, $\mathfrak{a} = \aleph_\alpha$). □

By VII.6.9, if $\mathrm{Lim}(\alpha)$ and $\mathrm{cf}(\aleph_\alpha) = \aleph_\alpha$, then $\mathrm{cf}(\alpha) = \aleph_\alpha \geq \alpha$ (the inequality holds by normality of $\aleph$). Hence

$$\aleph_\alpha = \alpha \tag{1}$$

since $\mathrm{cf}(\alpha) \leq \alpha$. So, what is the first fixed point $\alpha$ of $\aleph$? By VI.5.42–VI.5.43, that will be $\alpha = \sup\{s_n : n < \omega\}$, where

$$\begin{aligned} s_0 &= 0 \\ s_{n+1} &= \aleph_{s_n} \qquad \text{for } n > 0 \end{aligned}$$

This $\alpha$ is quite huge, namely,

$$\aleph_{\aleph_{\ddots_{\aleph_0}}}$$

On the other hand, $\mathrm{cf}(\alpha) = \omega$ for this $\alpha$, since $n \mapsto s_n$ is cofinal. Thus $\mathrm{cf}(\aleph_\alpha) = \mathrm{cf}(\alpha) = \omega < \aleph_\alpha$. We have just established that the first fixed point of $\aleph$, a huge limit cardinal, is *singular*. As this was only the first candidate for a weakly inaccessible cardinal, the first actual such cardinal will be even bigger, as it must occur later in the aleph sequence.

It turns out that within ZFC one cannot prove that weak inaccessibles exist. We will prove this relatively easy metamathematical fact below, but first we will need a notion of *strongly* inaccessible cardinals and some additional cardinal arithmetic tools.

**VII.6.14 Definition.** A cardinal $\mathfrak{a}$ is *strongly inaccessible*, or just *inaccessible*, iff it is weakly inaccessible and, moreover, for every infinite cardinal $\mathfrak{b} < \mathfrak{a}$, $2^{\mathfrak{b}} < \mathfrak{a}$. □

(1) Any cardinal $\mathfrak{a}$ that satisfies $\mathfrak{b} < \mathfrak{a} \to 2^{\mathfrak{b}} < \mathfrak{a}$ is called a *strong limit.*

(2) The above definition could also be phrased: "A cardinal $\mathfrak{a} > \aleph_0$ is *strongly inaccessible*, or just *inaccessible*, iff it is regular and, moreover, for every infinite cardinal $\mathfrak{b} < \mathfrak{a}, 2^{\mathfrak{b}} < \mathfrak{a}$." This is because for any $\mathfrak{b}$, $\mathfrak{b}^+ \leq 2^{\mathfrak{b}}$; thus the "moreover"

part yields the implication $\mathfrak{b} < \mathfrak{a} \to \mathfrak{b}^+ < \mathfrak{a}$; hence $\mathfrak{a}$ is a limit cardinal and therefore, in particular, weakly inaccessible.

In the presence of the generalized continuum hypothesis (GCH) that $2^{\mathfrak{b}} = \mathfrak{b}^+$ for all infinite cardinals, the requirement in VII.6.14 that $\mathfrak{b} < \mathfrak{a}$ implies $2^{\mathfrak{b}} < \mathfrak{a}$ is automatically satisfied, since $\mathfrak{a}$ is a limit cardinal. Thus, under GCH, weak and strong inaccessibles coincide.

A strongly inaccessible in comparison with other (smaller) infinite cardinals is like $\omega$ in comparison with smaller cardinals (natural numbers), since $n \in \omega$ implies $2^n \in \omega$.[†]

**VII.6.15 Definition (Generalized Cardinal Addition).** Let $(\mathfrak{k}_i)_{i \in I}$ be a family of cardinals. Their *sum*, $\sum_{i \in I} \mathfrak{k}_i$, is defined to be $\text{Card}(\bigcup_{i \in I}\{i\} \times \mathfrak{k}_i)$. □

Intuitively, in the sum we "count" all the elements in all the $\mathfrak{k}_i$ and allow for *multiplicity of occurrence* as well, since if $\mathfrak{k}_i = \mathfrak{k}_j$, still $\{i\} \times \mathfrak{k}_i \cap \{j\} \times \mathfrak{k}_j = \emptyset$.

**VII.6.16 Remark.** The above definition, a straightforward generalization of Definition VII.5.1, does not need AC, so it can be effected within ZF (with an appropriate definition of cardinals that also avoids AC). In ZFC it is equivalent to the commonly given statement (definitionally): "$\sum_{i \in I} \mathfrak{k}_i$ equals $\text{Card}(\bigcup_{i \in I} K_i)$, where $K_i \cap K_j = \emptyset$ whenever $i \neq j$, and $\mathfrak{k}_i = \text{Card}(K_i)$ for all $i \in I$."

Part of this is due to the obvious $\mathfrak{k}_i = \text{Card}(\{i\} \times \mathfrak{k}_i)$. The rest (including the immunity of the statement to the choice of $K_i$) follows from AC (the details will be left to the reader: Exercise VII.59). □

An interesting phenomenon occurs in connection with the above remark: $\sum_{i \in \aleph_0} \aleph_0$ (that is, $\sum_{i \in \aleph_0} \mathfrak{k}_i$ where every $\mathfrak{k}_i$ is $\aleph_0$) equals $\text{Card}(\bigcup_{i \in \aleph_0}\{i\} \times \aleph_0) = \text{Card}(\aleph_0^2) = \aleph_0$.

On the other hand, as we have noted a number of times before, Feferman and Levy (1963) have shown that, *in the absence of* AC, it is possible to have a countable family of mutually disjoint countable sets $(K_i)_{i \in I}$ such that $\text{Card}(\bigcup_{i \in I} K_i) = 2^{\aleph_0} > \aleph_0$. In lay terms, the "sum of the parts" can be significantly less than the "whole", without AC.

**VII.6.17 Proposition (Multiplication as Repeated Addition).** *For any cardinals* $\mathfrak{a}$ *and* $\mathfrak{b}$, $\mathfrak{a} \cdot_c \mathfrak{b} = \sum_{\alpha \in \mathfrak{a}} \mathfrak{b}$.

[†] "$2^n$" in the sense of Chapter V. This is the same as $2^{\cdot n}$.

*Proof.*

$$\sum_{\alpha\in\mathfrak{a}} \mathfrak{b} = \operatorname{Card}\left(\bigcup_{\alpha\in\mathfrak{a}} \{\alpha\} \times \mathfrak{b}\right)$$
$$= \operatorname{Card}(\mathfrak{a} \times \mathfrak{b}) = \mathfrak{a} \cdot_c \mathfrak{b} \qquad \square$$

**VII.6.18 Definition (Generalized Cardinal Multiplication).** Let $(\mathfrak{k}_i)_{i\in I}$ be a family of cardinals. Their *product* is defined to be $\operatorname{Card}(\prod_{i\in I} \mathfrak{k}_i)$. □

☡ We prefer not to propose a symbol for the product of a family of cardinal numbers, as there is no universal agreement. Of course, $\prod_{i\in I} \mathfrak{k}_i$ would be inappropriate, as it already indicates something else: the Cartesian product of the $\mathfrak{k}_i$.

If all the $\mathfrak{k}_i$ are equal to $\mathfrak{m}$, and $\operatorname{Card}(I) = \mathfrak{a}$, then $\operatorname{Card}(\prod_{i\in I} \mathfrak{k}_i) = \operatorname{Card}({}^I\mathfrak{m}) = \mathfrak{m}^{\mathfrak{a}}$. ☡

**VII.6.19 Remark.** If $A_i \sim B_i$ for $i \in I$, then $\prod_{i\in I} A_i \sim \prod_{i\in I} B_i$ (Exercise VII.64). □

**VII.6.20 Lemma (König).** *If* $\mathfrak{a}_i < \mathfrak{b}_i$ *for all* $i \in I$*, then*

$$\sum_{i\in I} \mathfrak{a}_i < \operatorname{Card}\left(\prod_{i\in I} \mathfrak{b}_i\right)$$

*Proof.* Set $A_i = \{i\} \times \mathfrak{a}_i$; thus

$$\sum_{i\in I} \mathfrak{a}_i = \operatorname{Card}\left(\bigcup_{i\in I} A_i\right)$$

$$\operatorname{Card}(A_i) = \mathfrak{a}_i \qquad \text{for } i \in I$$

and the $A_i$ are pairwise disjoint.

We need to show that there is *no* onto function

$$g : \bigcup_{i\in I} A_i \to \prod_{i\in I} \mathfrak{b}_i$$

Suppose otherwise. Set, for each $i \in I$,

$$B_i = g[A_i], \qquad \text{the image of } A_i \text{ under } g \tag{1}$$

Thus,

$$\prod_{i\in I} \mathfrak{b}_i = \bigcup_{i\in I} B_i$$

We next project $B_i$ along the $i$th coordinate to get

$$P_i = \{p(i) : p \in B_i\} \tag{2}$$

By (1), and the onto map $B_i \ni p \mapsto p(i) \in P_i$,

$$\begin{aligned} \mathrm{Card}(P_i) &\le \mathrm{Card}(B_i) \\ &\le \mathrm{Card}(A_i) \\ &< \mathfrak{b}_i \end{aligned}$$

Thus, $P_i \subset \mathfrak{b}_i$ ($P_i \subseteq \mathfrak{b}_i$, by (2)). Now, using AC, define a total $p$ on $I$ with $p(i) \in \mathfrak{b}_i - P_i$ for all $i \in I$. Clearly, $p \in \prod_{i\in I} \mathfrak{b}_i$, yet $p$ cannot be in $\mathrm{ran}(g)$, for, if so, $p \in B_i$ for some $i \in I$, and hence $p(i) \in P_i$; a contradiction. Thus, $g$ cannot be onto; a contradiction. □

König's lemma extends Cantor's diagonalization that lies behind Cantor's theorem. Indeed, $\mathfrak{a} = \sum_{\alpha\in\mathfrak{a}} 1 < \mathrm{Card}(\prod_{\alpha\in\mathfrak{a}} 2) = 2^{\mathfrak{a}}$.

**VII.6.21 Corollary.** *For all infinite cardinals* $\mathfrak{a}$, $\mathfrak{a} < \mathfrak{a}^{\mathrm{cf}(\mathfrak{a})}$.

*Proof.* Let $f : \mathrm{cf}(\mathfrak{a}) \to \mathfrak{a}$ be cofinal. Then

$$\begin{aligned} \mathfrak{a} &= \bigcup_{\beta<\mathrm{cf}(\mathfrak{a})} f(\beta) \\ &\le \sum_{\beta<\mathrm{cf}(\mathfrak{a})} \mathrm{Card}(f(\beta)) \quad \text{by Exercise VII.60} \\ &< \mathrm{Card}\left(\prod_{\beta<\mathrm{cf}(\mathfrak{a})} \mathfrak{a}\right) \quad \text{since } \mathrm{Card}(f(\beta)) \le f(\beta) < \mathfrak{a} \\ &= \mathfrak{a}^{\mathrm{cf}(\mathfrak{a})} \end{aligned}$$

□

**VII.6.22 Corollary.** $\mathrm{cf}(2^{\aleph_0}) > \aleph_0$.

Indeed, $\mathrm{cf}(2^{\aleph_\alpha}) > \aleph_\alpha$ for any $\alpha$ (see Exercise VII.65).

*Proof.* If we have equality, then (by VII.6.21) we get

$$2^{\aleph_0} < (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot_c \aleph_0} = 2^{\aleph_0}$$

□

In the absence of the CH, ZFC cannot pinpoint the cardinal $2^{\aleph_0}$ in the aleph sequence with any certainty. If $2^{\aleph_0} = \aleph_1$, then fine. But if not, then it can be (i.e., it is consistent with ZFC), as Cohen forcing has shown, that $2^{\aleph_0} = \aleph_2$ or $2^{\aleph_0} = \aleph_3$, or, indeed, that $2^{\aleph_0}$ is weakly inaccessible provided existence of such inaccessibles is consistent with ZFC.

However, we know that $2^{\aleph_0} \neq \aleph_\omega$ by VII.6.22, since $\mathrm{cf}(\aleph_\omega) = \aleph_0$.

**VII.6.23 Lemma.** *If* $\mathfrak{m} < \mathrm{cf}(\mathfrak{a})$*, then*

$$\mathfrak{a}^{\mathfrak{m}} = \sum_{\alpha<\mathfrak{a}} \mathrm{Card}(\alpha)^{\mathfrak{m}}$$

*Proof.* Trivially,

$$^{\mathfrak{m}}\mathfrak{a} \supseteq \bigcup_{\alpha<\mathfrak{a}} {}^{\mathfrak{m}}\alpha \tag{1}$$

Let next $f \in {}^{\mathfrak{m}}\mathfrak{a}$. By the assumption, $\sup \mathrm{ran}(f) < \mathfrak{a}$; hence $f \in \bigcup_{\alpha<\mathfrak{a}} {}^{\mathfrak{m}}\alpha$. Thus (1) is promoted to equality.

Next,

$$\begin{aligned}
\mathfrak{a}^{\mathfrak{m}} &= \mathrm{Card}\left(\bigcup_{\alpha<\mathfrak{a}} {}^{\mathfrak{m}}\alpha\right) \\
&\leq \sum_{\alpha<\mathfrak{a}} \mathrm{Card}(\alpha)^{\mathfrak{m}} && \text{by Exercise VII.60} \\
&= \mathfrak{a} \cdot_c \bigcup_{\alpha<\mathfrak{a}} \mathrm{Card}(\alpha)^{\mathfrak{m}} && \text{by Exercise VII.62} \\
&= \mathfrak{a}^{\mathfrak{m}} && \text{since } \mathrm{Card}(\alpha)^{\mathfrak{m}} \leq \mathfrak{a}^{\mathfrak{m}} \text{ for all } \alpha < \mathfrak{a}.
\end{aligned}$$

□

**VII.6.24 Corollary.** *If* $\mathfrak{a}$ *is regular and* $\mathfrak{m} < \mathfrak{a}$*, then*

$$\mathfrak{a}^{\mathfrak{m}} = \sum_{\alpha<\mathfrak{a}} \mathrm{Card}(\alpha)^{\mathfrak{m}}$$

**VII.6.25 Corollary (Hausdorff).** *For all* $\alpha, \beta$*,*

$$\aleph_{\alpha+1}^{\aleph_\beta} = \aleph_\alpha^{\aleph_\beta} \cdot_c \aleph_{\alpha+1}$$

*Proof.* For $\beta \le \alpha$ we apply VII.6.24 (see also VII.6.12 and VII.5.21) to obtain

$$\begin{aligned}
\aleph_{\alpha+1}^{\aleph_\beta} &= \sum_{\gamma \le \aleph_\alpha} \mathrm{Card}(\gamma)^{\aleph_\beta} \qquad \text{(note the "}\le\text{")} \\
&\le \sum_{\gamma \le \aleph_\alpha} \aleph_\alpha^{\aleph_\beta} \\
&= \aleph_\alpha^{\aleph_\beta} \cdot_c \aleph_{\alpha+1} \\
&\le \aleph_{\alpha+1}^{\aleph_\beta} \cdot_c \aleph_{\alpha+1} \\
&= \aleph_{\alpha+1}^{\aleph_\beta}
\end{aligned}$$

For $\alpha < \beta$ (hence also $\alpha + 1 \le \beta$) use Exercise VII.56 to obtain

$$\aleph_{\alpha+1}^{\aleph_\beta} = \aleph_\alpha^{\aleph_\beta} = 2^{\aleph_\beta}$$

Hence, from $\aleph_{\alpha+1} \le \aleph_\beta < 2^{\aleph_\beta}$ the contention becomes the following provable statement:

$$2^{\aleph_\beta} = 2^{\aleph_\beta} \cdot_c \aleph_{\alpha+1}$$

□

We conclude this excursion into "higher arithmetic" by noting how the adoption of GCH helps to further simplify cardinal arithmetic (in particular, exponentiation).

**VII.6.26 Proposition.** *If we adopt* GCH, *then*

$(i)$ $\aleph_\alpha^{\aleph_\beta} = \aleph_{\beta+1}$ *if* $\alpha \le \beta$,
$(ii)$ $\aleph_\alpha^{\aleph_\beta} = \aleph_{\alpha+1}$ *if* $\aleph_\alpha > \aleph_\beta \ge \mathrm{cf}(\aleph_\alpha)$,
$(iii)$ $\aleph_\alpha^{\aleph_\beta} = \aleph_\alpha$ *if* $\mathrm{cf}(\aleph_\alpha) > \aleph_\beta$.

*Proof.* $(i)$:

$$\begin{aligned}
\aleph_\alpha^{\aleph_\beta} &= 2^{\aleph_\beta} && \text{by Exercise VII.56} \\
&= \aleph_{\beta+1} && \text{by GCH}
\end{aligned}$$

$(ii)$:

$$\begin{aligned}
\aleph_{\alpha+1} &= \aleph_\alpha^{\aleph_\alpha} && \text{by } (i) \\
&\ge \aleph_\alpha^{\aleph_\beta} && \text{by Exercise VII.57} \\
&\ge \aleph_\alpha^{\mathrm{cf}(\aleph_\alpha)} && \text{by Exercise VII.57} \\
&> \aleph_\alpha && \text{by VII.6.21}
\end{aligned}$$

Thus, $\aleph_\alpha^{\aleph_\beta} = \aleph_{\alpha+1}$.

$(iii)$:

$$\begin{aligned}
\aleph_\alpha^{\aleph_\beta} &= \sum_{\gamma<\aleph_\alpha} \mathrm{Card}(\gamma)^{\aleph_\beta} && \text{by VII.6.23}\\
&= \aleph_\alpha \cdot_c \sup_{\gamma<\aleph_\alpha} \mathrm{Card}(\gamma)^{\aleph_\beta} && \text{by Exercise VII.62}
\end{aligned}$$

Now, for any $\gamma < \aleph_\alpha$,

$$\begin{aligned}
\mathrm{Card}(\gamma)^{\aleph_\beta} &= \mathrm{Card}({}^{\aleph_\beta}\gamma)\\
&\le \mathrm{Card}(\mathbf{P}(\aleph_\beta \times \gamma)) && \text{since } {}^{\aleph_\beta}\gamma \subseteq \mathbf{P}(\aleph_\beta \times \gamma)\\
&= 2^{\mathrm{Card}(\aleph_\beta \times \gamma)}\\
&= \mathrm{Card}(\aleph_\beta \times \gamma)^+ && \text{by GCH}\\
&= (\aleph_\beta \cdot_c \mathrm{Card}(\gamma))^+\\
&= \big(\max(\aleph_\beta, \mathrm{Card}(\gamma))\big)^+\\
&\le \aleph_\alpha
\end{aligned}$$

Thus, $\aleph_\alpha^{\aleph_\beta} = \aleph_\alpha$ in this case. □

We conclude this section by pondering the existence of inaccessibles.

**VII.6.27 Lemma.** *If $\alpha$ is strongly inaccessible and* $\mathrm{Card}(N) < \alpha$*, where $N$ is some arbitrarily chosen set of urelements, then* $\mathrm{Card}(V_N(\alpha)) = \alpha$.

*Proof.* Since $\alpha \subseteq V_N(\alpha)$ by VI.6.8,

$$\alpha = \mathrm{Card}(\alpha) \le \mathrm{Card}(V_N(\alpha)) \tag{1}$$

Since $\mathrm{Lim}(\alpha)$, $V_N(\alpha) = \bigcup_{\beta<\alpha} V_N(\beta)$. Thus,

$$\mathrm{Card}(V_N(\alpha)) \le \sum_{\beta<\alpha} \mathrm{Card}(V_N(\beta)) \le \alpha \cdot_c \sup(\mathrm{Card}(V_N(\beta))) \tag{2}$$

To conclude, by induction on $\beta$, we show that $\mathrm{Card}(V_N(\beta)) < \alpha$ for all $\beta < \alpha$.

If $\beta = 0$, then $\mathrm{Card}(V_N(\beta)) < \alpha$ from the choice of $N$.

If $\beta = \gamma + 1$, then

$$\begin{aligned}
\mathrm{Card}(V_N(\gamma + 1)) &= \mathrm{Card}(\mathbf{P}(N \cup V_N(\gamma)))\\
&\le 2^{\max(\mathrm{Card}(V_N(\gamma)),\, \mathrm{Card}(N))}\\
&< \alpha, && \text{by the I.H. and } \alpha\text{'s “strong limit” property.}
\end{aligned}$$

If $\mathrm{Lim}(\beta)$, then $V_N(\beta) = \bigcup_{\gamma\in\beta} V_N(\gamma)$. By the I.H., $\mathrm{Card}(V_N(\gamma)) < \alpha$ for $\gamma < \beta$; thus

$$\mathrm{Card}(V_N(\beta)) < \alpha, \qquad \text{by the I.H. and VII.6.11, since } \beta < \alpha.$$

Thus, (2) yields $\mathrm{Card}(V_N(\alpha)) \le \alpha$, and the result follows from (1). □

**VII.6.28 Lemma.** *If $\alpha$ is strongly inaccessible and* $\mathrm{Card}(N) < \alpha$, *where $N$ is some arbitrarily chosen set of urelements, then $A \subseteq V_N(\alpha)$ and* $\mathrm{Card}(A) < \mathrm{Card}(V_N(\alpha))$ *imply $A \in V_N(\alpha)$.*

*Proof.* Now, $V_N(\alpha) = \bigcup_{\beta<\alpha} V_N(\beta)$, $\mathrm{Card}(V_N(\alpha)) = \alpha$, and $\alpha$ is regular. By VII.6.10, $A \subseteq \bigcup_{\beta<\mathfrak{m}} V_N(\beta)$, where $\mathfrak{m} < \alpha$. Thus, $A \in V_N(\mathfrak{m}+1)$ (“ + 1” in the ordinal sense); hence $A \in V_N(\alpha)$. □

**VII.6.29 Lemma.** *If $\alpha$ is strongly inaccessible and* $\mathrm{Card}(N) < \alpha$, *where $N$ is some arbitrarily chosen set of urelements, then for a set $A$, $A \in V_N(\alpha)$ implies* $\mathrm{Card}(A) < \alpha$.

*Proof.* $A \in V_N(\alpha)$ implies $A \in V_N(\beta)$ for $\beta < \alpha$, and hence $A \subseteq N \cup V_N(\beta)$. Thus, $\mathrm{Card}(A) \leq \mathrm{Card}(N) +_c \mathrm{Card}(V_N(\beta)) < \alpha$, by the assumption (on $N$) and by the proof of VII.6.27. □

**VII.6.30 Theorem.** *If $\alpha$ is strongly inaccessible and* $\mathrm{Card}(N) < \alpha$, *where $N$ is some arbitrarily chosen set of urelements, then $V_N(\alpha)$ is a formal model of* ZFC.

*Proof.* The proof is very similar to the proof that $N \cup \mathbf{WF}_N$ is a model of ZFC (VI.6.13). Cf. also Sections VI.8 and VI.9. We prove that $\mathfrak{I} = (L_{\mathrm{Set}}, \mathrm{ZFC}, V_N(\alpha))$ is a formal model of ZFC. The verification then entails establishing $\vdash_{\mathrm{ZFC}} \mathscr{A}^{V_N(\alpha)}$ for the universal closure of each ZFC axiom.

Observe at the outset that $V_N(\alpha) = N \cup V_N(\alpha)$; hence it is transitive. It is also nonempty (why?)

(i) The axiom “$(\exists x)(\forall y)(U(y) \leftrightarrow y \in x)$” relativizes to “$(\exists x \in V_N(\alpha))(\forall y \in V_N(\alpha))(U(y) \leftrightarrow y \in x)$”. This is derivable (take $x = N$ and apply substitution axiom).

(ii) The axiom “$(\forall x)(U(x) \to (\forall y)y \notin x)$” relativizes to “$(\forall x \in V_N(\alpha))(U(x) \to (\forall y \in V_N(\alpha))y \notin x)$” and is a trivial consequence of the unrelativized version.

(iii) *Axiom of extensionality*. Derivable by VI.8.10.

(iv) *Axiom of separation*. It says that for any set $B$ and class $\mathbb{A}$, $\mathbb{A} \subseteq B$ implies that $\mathbb{A}$ is a set. To see why the relativization of this is derivable, let $B \in V_N(\alpha)$ and $\mathbb{A} \subseteq B$. By ZFC separation, $\mathbb{A}$ is a set. We need to prove that $(\mathbb{A} \text{ is a set})^{V_N(\alpha)}$, that is, $\mathbb{A} \in V_N(\alpha)$. Well, we have $\mathbb{A} \subseteq V_N(\alpha)$ by $\mathbb{A} \subseteq B$ and transitivity. Since (VII.6.29) $\mathrm{Card}(B) < \alpha$, we have $\mathrm{Card}(\mathbb{A}) < \alpha$ and are done by VII.6.28.

(v) *Axiom of foundation*. Holds by VI.8.11.

(vi) *Axiom of pairing*. For any $a, b$ in $V_N(\alpha)$ we must show the derivability of $((\exists y)y = \{a, b\})^{V_N(\alpha)}$. By VI.8.13 we need only show that $\{a, b\}^{V_N(\alpha)} \in V_N(\alpha)$, or that $\{a, b\} \in V_N(\alpha)$, by VI.8.2. Well,

$$\rho(\{a, b\}) = \max(\rho(a), \rho(b)) + 1 < \alpha$$

and this settles it.[†]

(vii) *Axiom of union*. For any *set of sets* $A \in V_N(\alpha)$ we need to show that

$$\left((\exists y)y = \bigcup A\right)^{V_N(\alpha)}$$

By VI.8.13, we need only show (using VI.8.16) that $\bigcup A \in V_N(\alpha)$. Well, let $A \in V_N(\beta)$ with $\beta < \alpha$. Then $\bigcup A \subseteq N \cup V_N(\beta)$, since $x \in A$ implies $x \in N \cup V_N(\beta)$ and thus $x \subseteq N \cup V_N(\beta)$. So $\rho(\bigcup A) \leq \max(0, \beta) + 1 < \alpha$.

(viii) *Power set axiom*. We need to show that for any *set* $A \in V_N(\alpha)$,

$$((\exists y)y = \mathbf{P}(A))^{V_N(\alpha)}$$

or that (VI.8.13)

$$\mathbf{P}^{V_N(\alpha)}(A) \in V_N(\alpha)$$

By absoluteness of $\subseteq$, $\mathbf{P}^{V_N(\alpha)}(A) = \mathbf{P}(A) \cap V_N(\alpha) = \mathbf{P}(A)$, the last equality because $x \subseteq A \in V_N(\beta)$ $(\beta < \alpha)$ implies $x \subseteq A \subseteq N \cup V_N(\beta)$, and hence $x \in V_N(\beta + 1)$. Thus, also, $\mathbf{P}(A) \subseteq \mathbf{P}(N \cup V_N(\beta))$; therefore $\mathbf{P}(A) \in V_N(\beta + 2)$.

(ix) *Collection*. For convenience, we approach collection via its equivalent form, *replacement*, that is, "For any set $A$ and any function $f$, $f[A]$ is a set." We need, therefore, to show that for any set $A \in V_N(\alpha)$ and any function $f \in V_N(\alpha)$

$$((\exists y)y = f[A])^{V_N(\alpha)}$$

or that $f[A] \in V_N(\alpha)$. Now, this is derivable by ZFC collection and VII.6.28, for $f \in V_N(\alpha)$ implies $f[A] \subseteq V_N(\alpha)$, and

$$\mathrm{Card}(f[A]) \leq \mathrm{Card}(A) \overset{\text{by VII.6.29}}{<} \alpha$$

(x) *Axiom of infinity*. We need an inductive set in $V_N(\alpha)$. Since $\omega \in V_N(\alpha)$, we are done.

[†] One can also do this with a sledgehammer: $\{a, b\} \subseteq V_N(\alpha)$ and $\mathrm{Card}(\{a, b\}) \leq 2 < \alpha$. Hence $\{a, b\} \in V_N(\alpha)$, by VI.6.28.

(xi) AC. Let $S$ be a set of nonempty sets in $V_N(\alpha)$. We need a choice function in $V_N(\alpha)$. By AC, there is a choice function, $f : S \to \bigcup S$, *in* ZFC, such that $f(x) \in x$ for all $x \in S$. Now by (viii), $\bigcup S \in V_N(\alpha)$; hence $S \times \bigcup S \in V_N(\alpha)$ (why?). Thus, $f \subseteq S \times \bigcup S$ implies $f \in V_N(\alpha)$. □

**VII.6.31 Theorem.** *It is consistent with* ZFC *that inaccessibles do not exist; that is, if* ZFC *is consistent, then so is* ZFC $+ \neg(\exists\alpha)(\alpha$ *is* (*strongly*) *inaccessible*).

*Proof.* (Metamathematical) It suffices to show that if ZFC is consistent, then

$$\text{ZFC} \nvdash (\exists\alpha)(\alpha \text{ is inaccessible})$$

Suppose instead that

$$\text{ZFC} \vdash (\exists\alpha)(\alpha \text{ is inaccessible}) \tag{1}$$

Then we have a proof in ZFC that the smallest inaccessible, $\beta$, exists. Now introduce new constants $\beta$ for that inaccessible, and $N$ for a set of urelements such that $\text{Card}(N) < \beta$.[†] Thus, $V_N(\beta)$ is a (formal) model of ZFC. By (1), I.7.9, and VII.6.30,

$$\text{ZFC} \vdash ((\exists\alpha)(\alpha \text{ is inaccessible}))^{V_N(\beta)}$$

or

$$\text{ZFC} \vdash (\exists\alpha \in V_N(\beta))(\alpha \text{ is inaccessible})^{V_N(\beta)} \tag{2}$$

Since "$\alpha$ is inaccessible" is absolute for $V_N(\beta)$ (see Exercise VII.71),[‡] it follows from (2) that there is a *real* inaccessible in $V_N(\beta)$, that is, (2) becomes

$$\text{ZFC} \vdash (\exists\alpha \in V_N(\beta))(\alpha \text{ is inaccessible})$$

which contradicts the choice of $\beta$ (see VI.6.9). Since ZFC is consistent, this contradiction establishes the original claim. □

**VII.6.32 Remark.** (1) The above can be transformed to a ZFC proof, via a formal model, that if ZFC is consistent, then so is ZFC $+ \neg(\exists\alpha)I(\alpha)$ (where we use "$I(\alpha)$" here as an abbreviation of "$\alpha$ is strongly inaccessible"). Once we fix $N$ with, say, $\text{Card}(N) \leq \omega$, the model is $\mathbb{M} = \{x : (\forall\alpha)(I(\alpha) \to x \in V_N(\alpha))\}$

[†] The reader has had enough practice by now to see that augmenting ZFC thus – including the relevant axioms, e.g., "$N$ is a set of atoms", "$\text{Card}(N) < \beta$", etc. – results in a conservative extension.

[‡] Intuitively, if $\alpha \in V_N(\beta)$, then an inhabitant of $V_N(\beta)$ will perceive it as a strongly inaccessible iff an inhabitant of $\mathbb{U}_N$ does.

with interpretation of $\in$, $U$ as themselves. This is clearly so, for there are two cases: If there are no inaccessibles (i.e., $\neg(\exists\alpha)I(\alpha)$), then $\mathbb{M} = \mathbb{U}_N$ is a model of ZFC $+\neg(\exists\alpha)I(\alpha)$; else $\mathbb{M} = V_N(\beta)$, where $\beta$ is the smallest inaccessible, and hence again (by VII.6.31) $\mathbb{M}$ is a model of ZFC $+\neg(\exists\alpha)I(\alpha)$ since $(\exists\alpha)I(\alpha)$ is false in $\mathbb{M}$(I.7.4).

(2) Can we, again in ZFC, prove consistency of ZFC $+(\exists\alpha)I(\alpha)$ (assuming consistency of ZFC)? No, because this would clash with Gödel's second incompleteness theorem, which says "In any extension $S$ of ZFC, if $S$ is recognizable *and* consistent, then $S \nvdash$ CONS($S$)", where CONS($S$) is a formula that says "$S$ is consistent". In outline, this goes like this. Assume that we have a proof

$$\text{ZFC} \vdash \text{CONS(ZFC)} \rightarrow \text{CONS(ZFC} + (\exists\alpha)I(\alpha)) \qquad (i)$$

Hence we also have a proof in the extension

$$\text{ZFC} + (\exists\alpha)I(\alpha) \vdash \text{CONS(ZFC)} \rightarrow \text{CONS(ZFC} + (\exists\alpha)I(\alpha)) \qquad (ii)$$

By VII.6.30,

$$\text{ZFC} + (\exists\alpha)I(\alpha) \vdash \text{CONS(ZFC)} \qquad (iii)$$

since, if $\beta$ is any inaccessible and Card($N$) $< \beta$, then for the universal closure $\mathscr{F}$ of every axiom of ZFC we have

$$\text{ZFC} + (\exists\alpha)I(\alpha) \vdash \mathscr{F}^{V_N(\beta)}$$

By $(ii)$, $(iii)$, and modus ponens we derive a contradiction to Gödel's incompleteness theorem:

$$\text{ZFC} + (\exists\alpha)I(\alpha) \vdash \text{CONS(ZFC} + (\exists\alpha)I(\alpha))$$

(3) How about weakly inaccessibles? Can we prove in ZFC (if this is consistent[†]) that weakly inaccessibles exist? Suppose we could. Then we could also prove this in the extension theory ZFC + GCH (which is also consistent – as Gödel has shown using his $\mathbb{L}$). If $\beta$ is the smallest weakly inaccessible as far as ZFC knows, then it is also the smallest *strongly* inaccessible in ZFC + GCH. But then $V_N(\beta)$, constructed in ZFC + GCH with a well-chosen $N$, is a model of ZFC. We have, as in VII.6.31,

$$\text{ZFC} + \text{GCH} \vdash (\exists\alpha \in V_N(\beta))I(\alpha)$$

a contradiction to the choice of $\beta$. □

[†] By now this hedging must have become annoying. However, recall that if ZFC is inconsistent, then for any formula $\mathscr{F}$ whatsoever, ZFC $\vdash \mathscr{F}$.

## VII.7. Inductively Defined Sets Revisited; Relative Consistency of GCH

We have had a first acquaintance, in VII.1.16, with

(1) sets defined inductively as *closures* under certain operations,
(2) induction *on inductively defined sets*, and
(3) the relation of this concept to that of set *operators*.

We now inform this discussion a bit further by our understanding of cardinals.

First let us expand our understanding of operation, so that we can now allow *infinitary* operations. This will have as a result, apart from the wider applicability of the concept (for example, the inductive definition of "computations in higher-type objects" involves infinitary operations) that the "operation" and "operator" approaches become equivalent (see the footnote to VII.1.31).

To this end, we will generalize operations, $f$, on a set $S$ so that they have as argument list any *set* of members from $S$, rather than a finite *sequence* of such objects. Before we proceed to formalize, let us make sure that this makes intuitive sense, that indeed the new way of looking at rules subsumes VII.1.15 and VII.1.16 as special cases.

How do we indicate *order* of arguments if the arguments are just lumped into a finite *set*? Well, an easy way to do this is to have many "rules" $X \mapsto x$ for any given input $X$, so that we incorporate all desirable outputs $x$ for all the relevant permutations of the set $X$ (a *permutation* of $X$ is, of course, a 1-1 correspondence from $X$ to $X$). For example, a rule $\lambda xy.x - y$ (for which order of arguments matters) would give rise to "rules" $\{x, y\} \mapsto x - y$ *and* $\{x, y\} \mapsto y - x$ for all $x, y$.

In general, an "old rule" (VII.1.15) on a set $S$, $\lambda \vec{a}_n.f(\vec{a}_n)$, will give rise in the present section to new rules

$$\{a_1, \ldots, a_n\} \mapsto f(a_{j_1}, \ldots, a_{j_n})$$

for all permutations $a_i \mapsto a_{j_i}$ of $\{a_1, \ldots, a_n\}$. In addition, we will allow rules $X \mapsto x$ with $X$ *possibly infinite*, thus going beyond simply translating VII.1.15 into new notation.

While we are at it, we find it elegant to allow rules $\emptyset \mapsto x$. The right hand sides of such rules ($x$) will play the role of the *initial objects* of VII.1.15. This will unify the discussion, avoiding the annoying asymmetry between rules and initial objects.

**VII.7.1 Definition.** A *rule set* $R$ on a given set $S$ is a relation $R \subseteq \mathbf{P}(S) \times S$. Instead of writing $\langle X, x\rangle \in R$ or $x\,RX$, we will prefer the notation $X \mapsto x$ or

$X \overset{R}{\mapsto} x$ if $R$ must be emphasized. A pair $\langle X, x\rangle$ or, in the preferred notation, $X \mapsto x$ will be called a *rule*.

A class $\mathbb{X}$ is $R$-closed iff whenever $A \subseteq \mathbb{X}$ then $R\langle A\rangle \subseteq \mathbb{X}$.

A rule set $R$ is *finitary* iff for all rules $X \mapsto x$ in $R$, $X$ is finite. Otherwise it is *infinitary*. □

☡ **VII.7.2 Remark.** A set $X$ is $R$-closed iff $R[\mathbf{P}(X)] \subseteq X$, since

$$R[\mathbf{P}(X)] = \{a : (\exists A)(a\; R\; A \wedge A \subseteq X)\}$$

□ ☡

**VII.7.3 Example.** Every ordinal is closed under the solitary rule $\emptyset \mapsto 0$.

Every limit ordinal is closed under the rule set

$$\begin{aligned} \emptyset &\mapsto 0 \\ \{\alpha\} &\mapsto \alpha + 1 \end{aligned}$$

□

It is clear that the rule sets are not single-valued relations in general. We will often omit mention of the set $S$ such that $R \subseteq \mathbf{P}(S) \times S$.

**VII.7.4 Definition.** Given a rule set $R$. We say that a set $X$ is *inductively,* or *recursively*, defined by $R$ iff $X$ is the $\subseteq$-smallest set that is $R$-closed.

Under these conditions, we also say that $X$ is *the closure* of $R$, in symbols $X = \mathrm{Cl}(R)$. □

As in VII.1.19, we have

**VII.7.5 Proposition.** *For any rule set $R$,* $\mathrm{Cl}(R)$ *is uniquely defined by*

$$\bigcap_{R[\mathbf{P}(X)] \subseteq X} X$$

*Proof. Uniqueness.* Say that $S$, $T$ are both candidates for $\mathrm{Cl}(R)$. Then $S \subseteq T$ and $T \subseteq S$ by VII.7.4; hence $S = T$.

*Existence.* To see that

$$S = \bigcap\{X : X \text{ is } R\text{-closed}\} \tag{1}$$

satisfies VII.7.4, observe that if $R$ is a rule *set*, then $\mathrm{ran}(R)$ is an $R$-closed *set*, and hence $\{X : X \text{ is } R\text{-closed}\} \neq \emptyset$, so that $S$ is a set. Trivially, the intersection of any set of $R$-closed sets is $R$-closed, so that $S$ is. Now, if $T \in \{X : X$ is $R$-closed$\}$, then $S \subseteq T$. □

**VII.7.6 Corollary (Induction on the Structure of Cl($R$), or $R$-Induction).** *Let $\mathscr{F}(x)$ be a formula, and $R$ a rule set. To prove that $(\forall x \in \mathrm{Cl}(R))\mathscr{F}(x)$, it suffices to prove that $\{x : \mathscr{F}(x)\}$ is $R$-closed.*

*Proof.* Suppose that $\{x : \mathscr{F}(x)\}$ is $R$-closed. Then so is $C = \{x : \mathscr{F}(x)\} \cap \mathrm{ran}(R)$. But $C$ is a set, hence $\mathrm{Cl}(R) \subseteq C \subseteq \{x : \mathscr{F}(x)\}$. □

**VII.7.7 Example.** Let $\mathscr{I}$ be a set of initial objects, and $\mathscr{F}$ a set of (function) operations on a set $S$, as in VII.1.15. Form a rule set $R$ as follows:

$$\emptyset \overset{R}{\mapsto} a \qquad \text{if } a \in \mathscr{I} \tag{1}$$

$$(\forall f \in \mathscr{F})(\{a_1, \ldots, a_n\} \overset{R}{\mapsto} f(a_{j_1}, \ldots, a_{j_n}) \\ \text{for all permutations } a_i \mapsto a_{j_i}) \tag{2}$$

where, in (2), $f(a_{j_1}, \ldots, a_{j_n}) \downarrow$ is understood.

We now see that $\mathrm{Cl}(\mathscr{I}, \mathscr{F}) = \mathrm{Cl}(R)$.

$\subseteq$: By VII.1.20, we need to show that $\mathrm{Cl}(R)$ is $\mathscr{F}$-closed and that $\mathscr{I} \subseteq \mathrm{Cl}(R)$. Now, since $\mathrm{Cl}(R)$ is $R$-closed, these contentions follow from (2) and (1) respectively. [For example, if $a_i \in \mathrm{Cl}(R)$ for $i = 1, \ldots, n$, and if $f(\vec{a}_n) \downarrow$ for $f \in \mathscr{F}$, then $f(\vec{a}_n) \in \mathrm{Cl}(R)$ by (2).]

$\supseteq$: By VII.7.6, we need to show that $\mathrm{Cl}(\mathscr{I}, \mathscr{F})$ is $R$-closed. So let

$$\mathrm{Cl}(\mathscr{I}, \mathscr{F}) \supseteq \{a_1, \ldots, a_n\} \overset{R}{\mapsto} a \tag{3}$$

By (2), the only way that (3) is possible is that $a = f(a_{j_1}, \ldots, a_{j_n})$ for some permutation of $a_1, \ldots, a_n$; hence $a \in \mathrm{Cl}(\mathscr{I}, \mathscr{F})$. We also need to settle the case

$$\mathrm{Cl}(\mathscr{I}, \mathscr{F}) \supseteq \emptyset \overset{R}{\mapsto} a \tag{4}$$

By (1) above, such $a$ are precisely those in $\mathscr{I}$; hence, again, $a \in \mathrm{Cl}(\mathscr{I}, \mathscr{F})$. □

We next relate $R$-induction to induction with respect to a well-founded relation $Q : A \to A$ ($A$ a set).

**VII.7.8 Example.** Let $Q : A \to A$ ($A$ a set) have IC, and define $R$ by

$$Q\langle x \rangle \overset{R}{\mapsto} x \qquad \text{for all } x \in A$$

Thus,

$$X \subseteq A \text{ is } R\text{-closed} \quad \text{iff} \quad Q\langle x \rangle \subseteq X \text{ implies } x \in X \tag{1}$$

Two remarks:

(i) By $Q$-induction (in the sense of VI.2.1), the right hand side of "iff" above says that $A \subseteq X$, and hence $A = X$.
(ii) Thus, by (1), since $\mathrm{Cl}(R) \subseteq A$ (why is $\mathrm{Cl}(R) \subseteq A$?) and $\mathrm{Cl}(R)$ is $R$-closed, we get that $A = \mathrm{Cl}(R)$.

A side effect is that instead of $Q$-induction, to prove properties of $A$ one can do $R$-induction. Indeed, the I.H. with respect to one relation is identical to that with respect to the other: For $Q$-induction we assume $Q\langle x\rangle \subseteq X$ (towards proving $x \in X$). For $R$-induction we want to show that $X$ is $R$-closed, but that, by (1), amounts again to assuming $Q\langle x\rangle \subseteq X$ (towards proving $x \in X$). □

**VII.7.9 Example (Some Pathologies).** Let $R$ be a rule set on a set $A$ given by $\{a\} \mapsto a$. Then every set $X$ is $R$-closed, so that $\emptyset = \mathrm{Cl}(R)$.

As another pathological case, let the rule set $R$ on set $B$ be such that whenever $X \overset{R}{\mapsto} x$, $X \neq \emptyset$. Now, $\mathrm{Cl}(R)$ exists anyhow, by VII.7.5. By VII.7.6 we can prove properties of $\mathrm{Cl}(R)$ by $R$-induction. This looks strange in view of VII.7.8, for one can start with *any* $Q : B \to B$, then define $R$ exactly as in VII.7.8, and lo and behold have an "induction tool" over $B$. Is the assumption that $Q$ has MC (or IC) on $B$ really important?

Yes. If not, one could end up with an $R$ as here described (due to the absence of $Q$-minimal elements). Under the circumstances, $\emptyset$ is $R$-closed; hence $\mathrm{Cl}(R) = \emptyset$, and we can do $R$-induction over $\emptyset$, *not* over $B$. Hardly an exciting prospect.

The moral is that:

(1) We cannot bring in induction over the entire field of $Q$ through the back door (via $R$ of VII.7.8), if $Q$ does not have IC on $B$. Our ability to do induction in these cases is restricted to some (often – as above – trivial) subset, $\mathrm{Cl}(R)$, of the field of $Q$ (see Exercise VII.73 for what we can say in the general case).
(2) To define "useful" closures, the rule set *must* have rules with empty premises ($\emptyset \mapsto a$). □

**VII.7.10 Definition (Immediate Predecessors, Ambiguity).** Let $R$ be a rule set. For each $a \in \mathrm{ran}(R)$ we define its *immediate predecessors* as follows:

If $\langle A, a\rangle \in R$, then $A$ is an *immediate predecessor set* (i.p.s.), while each member of $A$ is an *immediate predecessor* (i.p.), of $a$. If $\emptyset \mapsto a$ is the *only* rule involving $a$, then $a$ has no immediate predecessors.

The transitive closure of the i.p. relation is the *predecessor* relation.

If for some $a \in \mathrm{ran}(R)$ there are $A \neq B$ such that both $\langle A, a\rangle \in R$ and $\langle B, a\rangle \in R$, then $R$ is an *ambiguous* rule set; otherwise it is *unambiguous*.

Thus, $R$ is *un*ambiguous iff, for all $a \in \mathrm{ran}(R)$, $R^{-1}\langle a\rangle$ is a singleton (its sole member is the unique i.p.s. of $a$), in short, $R^{-1}$ is a function. □

Aczel (1978) calls what we termed ambiguous rule sets “nondeterministic” (Hinman (1978) calls them “non-monomorphic”). We prefer the above terminology, as it is consistent with its usage towards characterizing a related phenomenon in formal language theory. Similarly, the term “nondeterministic” is reserved in automata and language theory for rule sets that are not single-valued (as opposed to their *inverses* not being single-valued – which is what concerns us here).

**VII.7.11 Example.** Ambiguity makes it hard (often impossible) to define functions on $\mathrm{Cl}(R)$ the natural way, i.e., by induction on the formation of $\mathrm{Cl}(R)$. Here is an example.

Let us define symbol sequences using the symbols 1, 2, 3, +, × by the rule set $R$ given as follows:

$$\begin{aligned}
\emptyset &\mapsto 1\\
\emptyset &\mapsto 2\\
\emptyset &\mapsto 3\\
\{x, y\} &\mapsto x + y\\
\{x, y\} &\mapsto y + x\\
\{x, y\} &\mapsto x \times y\\
\{x, y\} &\mapsto y \times x
\end{aligned}$$

$\mathrm{Cl}(R)$ is the set of (strings denoting) non-parenthesized arithmetic expressions that utilize addition, multiplication, and the “constants” 1, 2, 3.

Suppose we want to define the *value*, $val(E)$ of any such expression, $E$. The natural way to do so is

$$\begin{aligned}
val(1) &= 1\\
val(2) &= 2\\
val(3) &= 3\\
val(x + y) &= val(x) + val(y) && \text{if } x, y \text{ are the i.p.'s of } x + y\\
val(x \times y) &= val(x) \times val(y) && \text{if } x, y \text{ are the i.p.'s of } x \times y
\end{aligned}$$

It should be clear that the above definition of $val$ is, intuitively, “ambiguous” or “ill-defined” (terminology that was formally adopted in VII.7.10). For example, there are *two* choices of i.p. sets for $1+2\times 3$. One choice is $x = 1+2$ and $y = 3$ (under $\times$), so that

$$\begin{aligned} val(1+2\times 3) &= val(1+2)\times val(3) \\ &= (val(1)+val(2))\times val(3) \\ &= (1+2)\times 3 = 9 \end{aligned}$$

while the other choice is $x = 1$ and $y = 2\times 3$ (under $+$), so that

$$\begin{aligned} val(1+2\times 3) &= val(1)+val(2\times 3) \\ &= val(1)+(val(2)\times val(3)) \\ &= 1+(2\times 3) = 7 \end{aligned}$$

We get different results! Even $1+2+3$ has two possible sets of i.p.'s, although this does not create a problem for *val*, since $+$ is commutative. □

It is not always easy to prove that a rule set is unambiguous (it is much easier, in general, to spot an ambiguity). The reader will be asked in the Exercises section to check that a few familiar rule sets are unambiguous (Exercises VII.74 to VII.77). Freedom from ambiguity is important in an inductive definition effected by a rule set $R$, for we can then "well-define", recursively, functions by induction over $\mathrm{Cl}(R)$. Examples of such functions are the *val* function over arithmetic expressions (assuming that arithmetic expressions are defined more carefully than in VII.7.11: brackets would have helped – see Exercise VII.75), the truth-value function on formulas (propositional calculus), assigning "meaning" (i.e., "interpretation" over some structure) to terms and formulas of a first order language, numerous definitions on "trees", and more. The following result allows such recursive definitions.

**VII.7.12 Example.** We continue on the theme of Example VII.7.8 by looking at the converse situation. Now we are given $A = \mathrm{Cl}(R)$, where $R$ is *unambiguous*. We define $Q : A \to A$ by

$$y\,Q\,x \quad \text{iff} \quad y \text{ is an i.p. of } x \text{ with respect to } R$$

Thus,

$$\text{if} \quad X \text{ is the (unique) i.p.s. of } x, \quad \text{then} \quad X = Q\langle x\rangle \tag{1}$$

Does $Q$ have IC? Well, suppose that $S$ is a set for which we know that

$$Q\langle x\rangle \subseteq S \to x \in S \tag{2}$$

Can we conclude that $A \subseteq S$? Indeed we can, as follows: Let $Y \subseteq S$ and $Y \overset{R}{\mapsto} y$. By (1), $Q\langle y\rangle = Y \subseteq S$. By (2), $y \in S$. Thus, $S$ is $R$-closed, hence $A \subseteq S$.

It follows that, for unambiguous $R$, $R$-induction can be replaced by i.p. induction (see however VII.7.9). □

**VII.7.13 Theorem (Recursion over a Closure).** *Let $R$ be an unambiguous rule set on a set $A$, and $g$ a total function on $A \times \mathbf{P}(A \times \operatorname{ran}(g))$. Then there is a unique total function $f$ on $\operatorname{Cl}(R)$ satisfying, for all $a \in \operatorname{Cl}(R)$,*

$$f(a) = g(a, f \restriction X_a) \qquad \textit{where } X_a \textit{ is the unique set such that } X_a \overset{R}{\mapsto} a$$

*Proof.* Define $Q$ on $\operatorname{Cl}(R)$ by

$$xQy \quad \text{iff} \quad x \in Y \overset{R}{\mapsto} y$$

Thus, for each $y \in \operatorname{Cl}(R)$, $Q\langle y\rangle$ is the unique i.p.s. of $y$, or

$$Y = Q\langle y\rangle \quad \text{iff} \quad Y \overset{R}{\mapsto} y$$

and the recurrence in the statement of the theorem becomes

$$f(a) = g(a, f \restriction Q\langle a\rangle)$$

Since $Q$ has IC on $\operatorname{Cl}(R)$ (by Example VII.7.12) we are done, via VI.2.28. □

Several variations are possible for VII.7.13 (see Section VI.2), but we will not pursue them here.

We return to operators $\Gamma : \mathbf{P}(X) \to \mathbf{P}(X)$ (Definition VII.1.25). It is now the case (compare with VII.1.31, footnote) that every *monotone* operator gives rise to an equivalent rule set.

**VII.7.14 Proposition.** *For every monotone operator $\Gamma : \mathbf{P}(X) \to \mathbf{P}(X)$ there is a rule set on $X$ such that $\overline{\Gamma} = \operatorname{Cl}(R)$.*

*Proof.* Define $R$ for each $A \subseteq X$, $a \in X$:

$$A \overset{R}{\mapsto} a \quad \text{iff} \quad a \in \Gamma(A) \tag{1}$$

Now, a set $Z \subseteq X$ is $R$-closed just in case $Z \supseteq A \mapsto a$ implies $a \in Z$. This, in view of (1) and monotonicity, says that

$$Z \subseteq X \text{ is } R\text{-closed} \quad \text{iff} \quad \Gamma(Z) \subseteq Z$$

As in VII.1.27,

$$\begin{aligned}\overline{\Gamma} &= \bigcap_{\substack{Z\subseteq X\\ \Gamma(Z)\subseteq Z}} Z\\ &= \bigcap_{\substack{Z\subseteq X\\ Z \text{ is } R\text{-closed}}} Z = \mathrm{Cl}(R)\end{aligned}$$

□

That, conversely, a rule set $R$ leads to a monotone operator $\Gamma$ such that $\mathrm{Cl}(R) = \overline{\Gamma}$ is proved as in VII.1.31, and we will not revisit it here. We conclude the section with the introduction of the *stages* of construction of $\overline{\Gamma}$, since, intuitively, what is happening is the *iteration* of a "construction"

```
$S \leftarrow \emptyset$
**repeat until** $S$ **converges to** $\overline{\Gamma}$
$S \leftarrow S \cup \Gamma(S)$
```

– that is, at each stage, we add to the $S$ that we have so far all the new points we constructed in $\Gamma(S)$ (cf. the "abstraction" of this in VI.5.47).

In the interest of greater flexibility in applying the operator concept, we relax the requirement that an operator $\Gamma$ be necessarily a set (viz., its left field and right field may be a proper class $\mathbb{X}$ whose members are sets).

**VII.7.15 Definition (Stages).** Let $\Gamma$ be a monotone operator, that is, possibly, a proper class total function that carries sets to sets. We define by recursion over On:

$$\Gamma^{\alpha} = \Gamma^{<\alpha} \cup \Gamma(\Gamma^{<\alpha})$$

where

$$\Gamma^{<\alpha} = \bigcup_{\beta<\alpha} \Gamma^{\beta}$$

for all $\alpha$.

We call the set $\Gamma^{\alpha}$ the $\alpha$th *stage* (often, by abuse of terminology, we refer to the ordinal $\alpha$ itself as the $\alpha$th stage). An element $s \in \Gamma^{\alpha}$ has *level* or *stage* $\leq \alpha$. It has level $\alpha$ if moreover $s \notin \Gamma^{\beta}$ for all $\beta < \alpha$. We write $\overline{\Gamma} = \bigcup_{\alpha} \Gamma^{\alpha}$ or $\Gamma^{\infty} = \bigcup_{\alpha} \Gamma^{\alpha}$. We call $\overline{\Gamma}$ ($\Gamma^{\infty}$) the *class inductively defined* by the operator $\Gamma$. □

The notation $\Gamma^{\alpha}$ might be confusing at first sight. This is the $\alpha$-th *set* constructed; it is not an operator. By the way, an easy induction on $\alpha$ shows that $\Gamma^{\alpha}$ is indeed a set (Exercise VII.78).

The notation $\Gamma^{<\alpha}$ for the union of all the stages before $\alpha$ is due to Moschovakis (it corresponds to the set $S$ we used in the pseudo-program above). Note that $\Gamma^{<0} = \emptyset$ and hence $\Gamma^0 = \Gamma(\emptyset)$.

**VII.7.16 Lemma.** *Let* $\Gamma$ *be any monotone operator* (not necessarily a set). *If, for some* $\alpha$, $\Gamma^{<\alpha} = \Gamma^\alpha$, *then:*

(1) $\overline{\Gamma} = \Gamma^\alpha = \Gamma^\beta$ *for* $\beta \geq \alpha$.
(2) $\overline{\Gamma}$ *is a fixed point of* $\Gamma$, *that is,* $\Gamma(\overline{\Gamma}) = \overline{\Gamma}$.

*Proof.* (1): Assume (I.H.) that $\alpha \leq \gamma < \beta$ implies $\Gamma^\alpha = \Gamma^\gamma$. Thus,

$$\begin{aligned}\Gamma^{<\beta} &= \bigcup_{\gamma<\beta} \Gamma^\gamma\\ &= \Gamma^{<\alpha} \cup \bigcup_{\alpha\leq\gamma<\beta} \Gamma^\gamma\\ &= \Gamma^{<\alpha} \cup \Gamma^\alpha \qquad \text{by I.H.}\\ &= \Gamma^{<\alpha} \qquad \text{by the choice of } \alpha\end{aligned}$$

Hence,

$$\begin{aligned}\Gamma^\beta &= \Gamma^{<\beta} \cup \Gamma(\Gamma^{<\beta})\\ &= \Gamma^{<\alpha} \cup \Gamma(\Gamma^{<\alpha})\\ &= \Gamma^\alpha\end{aligned}$$

In particular, $\overline{\Gamma} = \bigcup_\beta \Gamma^\beta = \Gamma^{<\alpha} = \Gamma^\alpha$, for the above $\alpha$.

As a by-product, $\overline{\Gamma}$ is a set.

(2): Since $\Gamma^\alpha = \Gamma^{<\alpha} \cup \Gamma(\Gamma^{<\alpha})$, it follows that $\Gamma(\Gamma^{<\alpha}) \subseteq \Gamma^\alpha$; hence,

$$\Gamma(\overline{\Gamma}) \subseteq \overline{\Gamma} \tag{$i$}$$

by $\overline{\Gamma} = \Gamma^\alpha = \Gamma^{<\alpha}$, with $\alpha$ as above. Next, as an I.H., assume that

$$\Gamma^{<\beta} \subseteq \Gamma(\overline{\Gamma})$$

Now,

$$\begin{aligned}\Gamma(\overline{\Gamma}) &= \Gamma\left(\bigcup_\gamma \Gamma^\gamma\right)\\ &\supseteq \Gamma\left(\bigcup_{\gamma<\beta} \Gamma^\gamma\right) \qquad \text{by monotonicity of } \Gamma. \qquad (ii)\end{aligned}$$

Thus, by I.H. and $(ii)$, $\Gamma^\beta = \Gamma^{<\beta} \cup \Gamma(\Gamma^{<\beta}) \subseteq \Gamma(\overline{\Gamma})$.

Therefore $\Gamma^{\beta} \subseteq \Gamma(\overline{\Gamma})$ for all $\beta$; hence $\overline{\Gamma} \subseteq \Gamma(\overline{\Gamma})$. This settles the issue, by $(i)$. □

**VII.7.17 Corollary.** *Let $X$ be a set, and $\Gamma : \mathbf{P}(X) \to \mathbf{P}(X)$ be a monotone operator. Then the following are provable (cf. VI.5.47):*

(1) $\overline{\Gamma}$ *is a set.*
(2) *There is an $\alpha$ such that $\Gamma^{<\alpha} = \Gamma^{\alpha}$. Moreover, $\overline{\Gamma} = \Gamma^{\alpha} = \Gamma^{\beta}$ for $\beta \geq \alpha$.*
(3) *The $\alpha$ of* (2) *satisfies* $\mathrm{Card}(\alpha) \leq \mathrm{Card}(X)$.
(4) $\overline{\Gamma}$ *is a fixed point of* $\Gamma$*, that is,* $\Gamma(\overline{\Gamma}) = \overline{\Gamma}$.

*Proof.* (1): This is trivial, since $\Gamma^{\alpha} \subseteq X$ for all $\alpha$, and hence $\overline{\Gamma} = \bigcup_{\alpha} \Gamma^{\alpha} \subseteq X$.

(2): By the proof of VI.5.47 (see also the remark following that proof). Alternatively, the function $f = \lambda s.\min\{\alpha : s \in \Gamma^{\alpha}\}$, that is, the one that maps each $s \in \overline{\Gamma}$ to its level, is a set by (1). Let $\alpha = \sup^{+} \mathrm{ran}(f)$. Then

$$\begin{aligned}\Gamma^{\alpha} &= \bigcup_{\beta<\alpha} \Gamma^{\beta} \cup \Gamma\left(\bigcup_{\beta<\alpha} \Gamma^{\beta}\right)\\ &= \bigcup_{\beta<\alpha} \Gamma^{\beta} \qquad \text{since every } s \in \Gamma(\Gamma^{<\alpha}) \text{ is in some } \Gamma^{\beta},\ \beta < \alpha\\ &= \Gamma^{<\alpha}\end{aligned}$$

The rest follows from VII.7.16.

(3): Since the function $f : \overline{\Gamma} \to \alpha$ of (2) is onto, and $\overline{\Gamma} \subseteq X$, it follows that $\mathrm{Card}(\alpha) \leq \mathrm{Card}(\overline{\Gamma}) \leq \mathrm{Card}(X)$.

(4): From VII.7.16. □

**VII.7.18 Remark.** (1) For an arbitrary monotone operator $\Gamma$, the smallest $\alpha$ such that $\Gamma^{<\alpha} = \Gamma^{\alpha} = \overline{\Gamma}$, *if it exists*, is called the ordinal of $\Gamma$ and is often denoted by $|\Gamma|$.

(2) We next relax the concept of rule set to allow also (proper) rule *classes*. However, we require some restriction on the size of the left hand sides of rules. □

**VII.7.19 Definition.** An $\mathfrak{m}$-*based rule class* (possibly proper) $\mathbb{R}$, where $\mathfrak{m}$ is regular, is a left narrow class of rules such that for every rule $A \mapsto a$ of $\mathbb{R}$, we have $\mathrm{Card}(A) < \mathfrak{m}$. An $\omega$-based rule is called *finitary*. □

**VII.7.20 Proposition.** *If $\Gamma$ is a monotone operator* (*possibly a proper class*) *defined from an $\mathfrak{m}$-based rule class $\mathbb{R}$ by $\Gamma(A) = \{x : (\exists Y \subseteq A) Y \overset{\mathbb{R}}{\mapsto} x\}$ for all*

*A, then*

(1) $|\Gamma| \le \mathfrak{m}$,
(2) $\mathrm{Cl}(\mathbb{R}) = \overline{\Gamma}$.

$\Gamma(A)$ is a set by left narrowness.

*Proof.* (1): Since $\Gamma^{\mathfrak{m}} \supseteq \Gamma^{<\mathfrak{m}}$, it suffices to show that $\Gamma^{\mathfrak{m}} \subseteq \Gamma^{<\mathfrak{m}}$. Let then $x \in \Gamma^{\mathfrak{m}}$. Thus, either $x \in \Gamma^{<\mathfrak{m}}$, in which case there is nothing to prove, or $x \in \Gamma(\Gamma^{<\mathfrak{m}})$. Thus, for some $A \subseteq \Gamma^{<\mathfrak{m}}$, we have $\mathrm{Card}(A) < \mathfrak{m}$ and $A \mapsto x$ is an $\mathbb{R}$-rule. By VII.6.10, $A \subseteq \Gamma^{<\alpha}$ for some $\alpha < \mathfrak{m}$; thus $x \in \Gamma(\Gamma^{<\alpha}) \subseteq \Gamma^{<\mathfrak{m}}$.

(2): By VII.7.16, $\Gamma(\overline{\Gamma}) = \overline{\Gamma} = \Gamma^{\mathfrak{m}}$. Thus, $\overline{\Gamma}$ is an $\mathbb{R}$-closed *set*; hence $\mathrm{Cl}(\mathbb{R})$ exists (i.e., is a set). Indeed,

$$\mathrm{Cl}(\mathbb{R}) \subseteq \overline{\Gamma} \tag{$i$}$$

On the other hand, assume $\Gamma^{<\alpha} \subseteq \mathrm{Cl}(\mathbb{R})$. It follows ($\mathrm{Cl}(\mathbb{R})$ is $\mathbb{R}$-closed) that

$$\Gamma(\Gamma^{<\alpha}) \subseteq \mathrm{Cl}(\mathbb{R})$$

and hence (by induction)

$$\Gamma^{\alpha} \subseteq \mathrm{Cl}(\mathbb{R}) \qquad \text{for all } \alpha$$

which promotes $(i)$ to equality. □

We apply these ideas to prove the important *reflection principle*.

**VII.7.21 Lemma.** *For any formula $\mathscr{F}(y, \vec{x}_n)$ and set $N$, there is a set $M \supseteq N$ such that:*

(1) *The following is provable:*

$$u_1 \in M \wedge \cdots \wedge u_n \in M \to \Big((\exists y)\mathscr{F}(y, \vec{u}_n) \leftrightarrow (\exists y \in M)\mathscr{F}(y, \vec{u}_n)\Big)$$

*and*

(2) *$M$ can be chosen to satisfy* $\mathrm{Card}(M) \le \max(\mathrm{Card}(N), \aleph_0)$.

*Proof.* (1): Define the $\omega$-based rule class

$$\mathbb{R} = \Big\{\{u_1, \ldots, u_n\} \mapsto y : \mathscr{F}(y, \vec{u}_n) \wedge y \text{ has least rank}\Big\} \cup \{\emptyset \mapsto x : x \in N\}$$

$M = \mathrm{Cl}(\mathbb{R})$ is a set (by VII.7.20), satisfying $N \subseteq M$.

Let us take $u_i$, $i = 1, \ldots, n$, in $M$. The $\leftarrow$-direction of (1) is trivial. Let then

$$(\exists y)\mathscr{F}(y, \vec{u}) \tag{$i$}$$

Thus we may add $\mathscr{F}(a, \vec{u})$, where $a$ is a new constant and $\rho(a)$ is minimum. Since $M$ is $\mathbb{R}$-closed, $a \in M$; thus $(\exists y \in M)\mathscr{F}(y, \vec{u})$ by substitution axiom.

(2): Using AC, cut $\mathbb{R}$ down to $T$ such that for each of the $n!$ permutations $\vec{w}$ of $u_1, \ldots, u_n$, where $u_i \in M$ (*the $M$* above) we keep a *unique* $\{u_1, \ldots, u_n\} \mapsto y$ whenever $\mathscr{F}(y, \vec{w})$ (this $T$ is, of course, a set). Set $M' = \mathrm{Cl}(T)$.

First of all, for all $u_i \in M'$, $(\exists y)\mathscr{F}(y, \vec{u}) \leftrightarrow (\exists y \in M')\mathscr{F}(y, \vec{u})$, exactly as in (1). Next, by VII.7.20,

$$M' = \bigcup_{p \in \omega} \Gamma^p \tag{$ii$}$$

where $\Gamma$ is the monotone operator associated with the rule *set* $T$ (recall, $T$ is $\omega$-based, whence the choice of upper bound of $\bigcup$ in $(ii)$).

By induction on $p$ we argue that $\mathrm{Card}(\Gamma^p) \leq \max(\mathrm{Card}(N), \aleph_0)$. Indeed, this is true for $p = 0$, as $\Gamma^0 = \Gamma(\Gamma^{<0}) = \Gamma(\emptyset) = N$. Now,

$$\begin{aligned}\mathrm{Card}(\Gamma^{p+1}) &= \mathrm{Card}\left(\bigcup_{i \leq p} \Gamma^i \cup \Gamma\left(\bigcup_{i \leq p} \Gamma^i\right)\right)\\ &\leq \mathrm{Card}\left(\bigcup_{i \leq p} \Gamma^i\right) +_c \mathrm{Card}\left(\Gamma\left(\bigcup_{i \leq p} \Gamma^i\right)\right) \end{aligned}\tag{$iii$}$$

By the I.H.,

$$\mathrm{Card}\left(\bigcup_{i \leq p} \Gamma^i\right) \leq (p+1) \cdot_c \max(\mathrm{Card}(N), \aleph_0) = \max(\mathrm{Card}(N), \aleph_0) \tag{$iv$}$$

Also, setting $S = \bigcup_{i \leq p} \Gamma^i$,

$$\begin{aligned}\mathrm{Card}\big(\Gamma(S)\big) &= \mathrm{Card}\big(\{y : (\exists \vec{u} \in S)(\{u_1, \ldots, u_n\} \mapsto y \text{ is in } T)\}\big)\\ &\leq \big(\mathrm{Card}(S)\big)^n \qquad \text{since } T \text{ is single-valued in } y\\ &\leq \max(\mathrm{Card}(N), \aleph_0) \qquad \text{by } (iv)\end{aligned}\tag{$v$}$$

By $(iii)$–$(v)$ the induction is complete. Thus, by $(ii)$,

$$\mathrm{Card}(M') \leq \aleph_0 \cdot_c \max(\mathrm{Card}(N), \aleph_0) = \max(\mathrm{Card}(N), \aleph_0) \qquad \square$$

**VII.7.22 Corollary.** *Lemma* VII.7.21 *holds if we have a finite number of formulas $\mathscr{F}_i$, $i = 1, \ldots, m$. That is, for any set $N$, there is a set $M \supseteq N$ such that:*

(1) *The following is provable for each $i = 1, \ldots, m$:*

$$u_1 \in M \wedge \cdots \wedge u_{i_k} \in M \to \Big((\exists y)\mathscr{F}_i(y, \vec{u}_{i_k}) \leftrightarrow (\exists y \in M)\mathscr{F}_i(y, \vec{u}_{i_k})\Big)$$

*and*

(2) *$M$ can be chosen to satisfy* $\mathrm{Card}(M) \leq \max(\mathrm{Card}(N), \aleph_0)$.

Lemma VII.7.21 also holds for any set of formulas that can be *indexed within the theory*. However, for an arbitrary (infinite) set of formulas (not indexed within the theory) the lemma breaks down. It is still true *metamathematically*, though, since, arguing in the *metatheory*, we can index this (enumerable) set of formulas using $\mathbb{N}$ as index set. Of course, the $\mathbb{R}$ so obtained (by "put $\{u_1, \ldots, u_n\} \mapsto y$ in $\mathbb{R}$ as long as $\mathscr{G}_i(y, \vec{u})$ for some $i \in \mathbb{N}$, and $y$ has least rank") is still $\omega$-based.

The proof technique in VII.7.21 (and the flavour of the result in VII.7.23) is analogous to that employed towards the *downward Löwenheim-Skolem theorem* of model theory (proved in volume 1 of these lectures).

We next apply VII.7.22 to show that for any finite set of formulas, there is a set $M$ such that each of these formulas is absolute for $M$. We say that $M$ *reflects* these formulas.

**VII.7.23 Theorem (Reflection Principle).** *For any set $N$ and any finite set of formulas $\mathscr{F}_i$, $i = 1, \ldots, m$, there is a set $M \supseteq N$ such that*

$$\text{ZFC} \vdash \mathscr{F}_i \leftrightarrow \mathscr{F}_i^M \qquad \textit{for } i = 1, \ldots, m$$

*assuming $u_k \in M$ for all the free variables $u_k$.*

*Moreover, an $M$ with cardinality at most* $\max(\text{Card}(N), \aleph_0)$ *exists.*

*Proof.* Let $\mathscr{G}_j$, $j = 1, \ldots, r$, be the list of all formulas that consists of the list $\mathscr{F}_i, i = 1, \ldots, m$, augmented by *all subformulas of the $\mathscr{F}_i$*. If none of the $\mathscr{G}_j$ is of the form $(\exists y)\mathscr{Q}$, then take $M = N$. Otherwise, take $M \supseteq N$, using VII.7.22 on all formulas of the form $(\exists y)\mathscr{Q}$ in the $\mathscr{G}_j$-list.

By induction on formulas we show next that

$$\text{ZFC} \vdash \mathscr{G}_j \leftrightarrow \mathscr{G}_j^M \qquad \text{for } j = 1, \ldots, r \tag{1}$$

from which the theorem follows.

If $\mathscr{G}_j$ is atomic, then (1) follows by VI.8.1 if any $a \in N$, added as a constant to $L_{\text{Set}}$, relativizes as $a$. If $\mathscr{G}_j$ is $\neg\mathscr{A}$ or $\mathscr{A} \vee \mathscr{B}$, then the I.H. guarantees that

$$\text{ZFC} \vdash \mathscr{A} \leftrightarrow \mathscr{A}^M$$

and

$$\text{ZFC} \vdash \mathscr{B} \leftrightarrow \mathscr{B}^M$$

from which, using VI.8.1 and the Leibniz rule, we get

$$\text{ZFC} \vdash \neg\mathscr{A} \leftrightarrow (\neg\mathscr{A})^M$$

and

$$\text{ZFC} \vdash \mathscr{A} \vee \mathscr{B} \leftrightarrow (\mathscr{A} \vee \mathscr{B})^M$$

Finally, let $\mathscr{G}_j$ be $(\exists y)\mathscr{Q}$. We get

$$\begin{aligned}\text{ZFC} \vdash (\exists y)\mathscr{Q} &\leftrightarrow (\exists y \in M)\mathscr{Q} && \text{by VII.7.22}\\ &\leftrightarrow (\exists y \in M)\mathscr{Q}^M && \text{by I.H. and Leibniz rule}\\ &\leftrightarrow \big((\exists y)\mathscr{Q}\big)^M && \text{by VI.8.1}\end{aligned}$$

(1) is proved, and we are done. □

A consequence of the reflection principle is that ZFC cannot be finitely axiomatized if it is consistent.[†] That is, there is *no* finite set of sentences $\mathscr{F}_i$, $i = 1, \ldots, n$, such that for every formula $\mathscr{Q}$,

$$\text{ZFC} \vdash \mathscr{Q} \quad \text{iff} \quad \mathscr{F}_1, \ldots \mathscr{F}_n \vdash \mathscr{Q}. \tag{1}$$

This is so because a consistent ZFC using (1) can prove the existence of a (set) model for itself (i.e., one for $\{\mathscr{F}_1, \ldots, \mathscr{F}_n\}$). Thus, ZFC can prove its consistency (cf. I.7.8):

$$\text{ZFC} \vdash (\exists M)(\neg U(M) \wedge \mathscr{F}_1^M \wedge \cdots \wedge \mathscr{F}_n^M)$$

by VII.7.23 and tautological implication[‡] with help from the Leibniz rule. This is contrary to Gödel's second incompleteness theorem.

As a by-product of this observation, we also conclude that an extension of VII.7.21 to an arbitrary set of formulas not only does not follow (in ZFC) from our (Löwenheim-Skolem) proof technique, but is downright impossible.

Now, working in the metatheory, we can mimic the construction that builds the model $\mathbb{U}_A$ for some set of urelements $A$. Continuing in the metatheory, we can apply reflection (to the enumerable – in the metatheory – set of axioms) and "cut $\mathbb{U}_A$ down" to an enumerable $(U, \in)$-model $(M, U, \in)$.[§] We can next apply Mostowski collapsing ($\lambda x.C(M, x) : M \to C(M, M)$; see VI.2.38, p. 312) to get an $\in$-isomorphic *transitive* set structure $(C(M, M), U, \in)$ which is also a model, since $\lambda x.C(M, x)$ preserves atoms and the $\in$-relation.[¶]

[†] ZFC, as given, indeed has infinitely many axioms. For example, collection provides one axiom for each formula $\mathscr{F}$. On the other hand, if ZFC is inconsistent, then certainly all its theorems (which happen to be *all formulas* under these circumstances) follow from the single axiom $(\forall x)x \neq x$.

[‡] If ZFC $\vdash A \leftrightarrow A^M$ and ZFC $\vdash A$, then ZFC $\vdash A^M$.

[§] Take $N$ in the proof of VII.7.23 to be enumerable.

[¶] See VI.2.36–VI.2.39. Of course, $M$ is extensional, being a ZFC $(U, \in)$-model.

Thus, Platonistically, we have shown that a so-called *countable transitive model* (CTM) – $(C(M, M), U, \in)$ – for ZFC exists.

This provides the source for the so-called "Skolem paradox" (not a real paradox): In ZFC we can prove the existence of sets of enormous cardinality. In particular, we can prove (Cantor's theorem) that

$$\omega \not\sim \mathbf{P}(\omega) \tag{1}$$

However, it is "really true" that

$$\omega^{C(M,M)} \sim \mathbf{P}(\omega)^{C(M,M)} \tag{2}$$

since both sets are enumerable. Isn't this a contradiction?

We know better by now. (2) is irrelevant, for it is not equivalent to $(\omega \sim \mathbf{P}(\omega))^{C(M,M)}$, due to the presence of an unbounded existential quantifier. As far as an inhabitant of $C(M, M)$ is concerned, he sees that

$$\models_{C(M,M)} \omega \not\sim \mathbf{P}(\omega)$$

and this is as it should be by (1). This person cannot see the 1-1 correspondence $f$ that effects (2), for $f$ is *not* in $C(M, M)$. Note that the expression immediately above says the same thing as (cf. VI.8.4)

$$\models_{\mathbb{U}_N} \big(\omega \not\sim \mathbf{P}(\omega)\big)^{C(M,M)}$$

**Consistency of GCH with ZF.** We conclude this chapter with a proof that $\mathbb{L}_N$ is a model of GCH. Which $\mathbb{L}_N$? We add to ZF the new constants $N$, $f$ and the axiom

$$\neg U(N) \wedge (\forall z \in N)U(z) \wedge f \text{ is a 1-1 function} \wedge \text{dom}(f) \subseteq \omega \wedge \text{ran}(f) = N$$

To avoid unnecessary linguistic (and notational) acrobatics *we call this conservative extension of* ZF *just* ZF. Then we build $\mathbb{L}_N$ in ZF as before.

We also bypass tedious relativizations to $\mathbb{L}_N$ by working in $\text{ZF} + (\mathbb{V} = \mathbb{L})$ or a conservative extension thereof throughout (cf. VI.9.18). Thus, rather than proving $\vdash_{\text{ZF}} \text{GCH}^{\mathbb{L}_N}$, we prove GCH in $\text{ZF} + (\mathbb{V} = \mathbb{L})$ instead. The key lemma is the following:

**VII.7.24 Lemma.** *In* $\text{ZF} + (\mathbb{V} = \mathbb{L})$ *we can prove that if $A$ is a transitive set and* $\text{Card}(A) \leq \aleph_\alpha$, *then* $A \subseteq \{F_\beta : \beta < \aleph_{\alpha+1}\}$.

Once the above is settled, one can easily prove:

**VII.7.25 Theorem.** GCH *is provable in* $\mathrm{ZF}+(\mathbb{V}=\mathbb{L})$.

*Proof.* Let $S \subseteq \aleph_\alpha$. Thus, $A=\aleph_\alpha \cup \{S\}$ is transitive, for $x \in A$ leads to two cases: $x=S$ (and we are done by $S \subseteq \aleph_\alpha$), or $x \in \aleph_\alpha$ (but $\aleph_\alpha$ is transitive). Moreover, $\mathrm{Card}(A) \leq \aleph_\alpha +_c 1 = \aleph_\alpha$. Thus, $A \subseteq \{F_\beta : \beta < \aleph_{\alpha+1}\}$ by VII.7.24, from which

$$S \in \{F_\beta : \beta < \aleph_{\alpha+1}\}$$

Therefore

$$\mathbf{P}(\aleph_\alpha) \subseteq \{F_\beta : \beta < \aleph_{\alpha+1}\}$$

Hence

$$\mathrm{Card}\big(\mathbf{P}(\aleph_\alpha)\big) \leq \mathrm{Card}\big(\{F_\beta : \beta < \aleph_{\alpha+1}\}\big) \leq \aleph_{\alpha+1}$$

– the last $\leq$ due to the onto map $\aleph_{\alpha+1} \ni \beta \mapsto F_\beta$. Since $\aleph_{\alpha+1} \leq \mathrm{Card}\big(\mathbf{P}(\aleph_\alpha)\big)$, we are done. □

**VII.7.26 Corollary.** *If* ZF *is consistent, then so are* $\mathrm{ZF}+\mathrm{GCH}$ *and* $\mathrm{ZFC}+\mathrm{GCH}$.

*Proof of Lemma VII.7.24.* Recall that, working in $\mathrm{ZF}+(\mathbb{V}=\mathbb{L})$, we get AC for free; therefore all our work on cardinals is available to us. The proof is an application of reflection followed by Mostowski collapsing. Freeze then sets $A$ and $\mathfrak{m}$ along with the assumptions

$$A \text{ is transitive and } \mathrm{Card}(A) \leq \mathfrak{m},\ \mathfrak{m} \text{ being an infinite cardinal}^\dagger \tag{1}$$

It is convenient to work in a conservative extension $\mathfrak{T}$ of $\mathrm{ZF}+(\mathbb{V}=\mathbb{L})$ for a while.

Let us denote by $L$ the language of $\mathrm{ZF}+(\mathbb{V}=\mathbb{L})$ (this includes the constants $N$ and $f$). $\mathfrak{T}$ is obtained from $\mathrm{ZF}+(\mathbb{V}=\mathbb{L})$ by adding to $L$ a new constant $B$ and the axioms

$$\{f,N\} \cup N \cup TC(f) \cup A \subseteq B \wedge \neg U(B) \tag{2}$$

$$\mathrm{Card}(B) \leq \mathfrak{m} \tag{3}$$

[†] Recall that "freezing", jargon we have applied constantly towards invoking the deduction theorem, formally means to add new set constants, $A$ and $\mathfrak{m}$, and the assumptions (1).

and the schema

$$\mathscr{A} \leftrightarrow \mathscr{A}^B \qquad \text{for every sentence } \mathscr{A} \text{ of } L \tag{4}$$

where $N^B = N$ and $f^B = f$. Note that (2) and (3) are relatively consistent by (1) and the choice of $N$.

To see that $\mathfrak{T}$ is as claimed, let $\vdash_{\mathfrak{T}} \mathscr{A}$, where $\mathscr{A}$ is over $L$. Fix attention to one such proof, and let $\mathscr{F}_1, \ldots, \mathscr{F}_n$ be the universal closures of all the axioms among (2)–(4) appearing in it. Thus, $\mathrm{ZF} + (\mathbb{V} = \mathbb{L})$ – *although, over an extended language* $L'$ *that includes the constant* $B$ – proves

$$\mathscr{F}_1 \wedge \cdots \wedge \mathscr{F}_n \rightarrow \mathscr{A} \tag{5}$$

by the deduction theorem. Therefore (cf. I.4.16), we have a proof in $\mathrm{ZF} + (\mathbb{V} = \mathbb{L})$ of $\mathscr{F}'_1 \wedge \cdots \wedge \mathscr{F}'_n \rightarrow \mathscr{A}$ – this formula being over $L$ – where $\mathscr{F}'_i$ is obtained from $\mathscr{F}_i$ by replacing all occurrences of $B$ in it by a new variable $z$ (the same $z$ is used in all the $\mathscr{F}_i$) that does not occur as either free or bound in (5). By $\exists$-introduction,

$$\vdash_{\mathrm{ZF}+(\mathbb{V}=\mathbb{L})} (\exists z)(\mathscr{F}'_1 \wedge \cdots \wedge \mathscr{F}'_n) \rightarrow \mathscr{A} \tag{6}$$

However,

$$\vdash_{\mathrm{ZF}+(\mathbb{V}=\mathbb{L})} (\exists z)(\mathscr{F}'_1 \wedge \cdots \wedge \mathscr{F}'_n)$$

by VII.7.23 and $\mathrm{Card}(\{f, N\} \cup N \cup TC(f) \cup A) \leq \mathfrak{m}$ by $N$ being countable. VII.7.23 is applicable because only finitely many sentences (from schema (4)) are involved in $\mathscr{F}'_1 \wedge \cdots \wedge \mathscr{F}'_n$. By (6) we now have a proof of $\mathscr{A}$ in $\mathrm{ZF} + (\mathbb{V} = \mathbb{L})$ which establishes the conservative nature of the extension $\mathfrak{T}$.

$\mathfrak{I} = (L', \mathfrak{T}, B)$ is a formal $(U, \in)$-model of $\mathrm{ZF} + (\mathbb{V} = \mathbb{L})$, where $L'$ is $L$ with the addition of $B$. Indeed, if $\mathscr{F}$ is the universal closure of a $\mathrm{ZF} + (\mathbb{V} = \mathbb{L})$ axiom, then $\vdash_{\mathfrak{T}} \mathscr{F}$, since $\mathfrak{T}$ is an extension of $\mathrm{ZF} + (\mathbb{V} = \mathbb{L})$. By (4), $\vdash_{\mathfrak{T}} \mathscr{F}^B$.

We prefer to have a transitive (set) model, so we invoke Mostowski collapsing (cf. VI.2.38). Since $B$ (*argot* for $\mathfrak{I}$) is a model of $\mathrm{ZF} + (\mathbb{V} = \mathbb{L})$, it satisfies, in particular, extensionality. That is, it is *extensional* in the sense of VI.2.38. We have shown there that the unary function $\phi$ *introduced* in the theory $\mathfrak{T}$ over $L'$ by the recursive definition[†]

$$\phi(x) = \begin{cases} x & \text{if } U(x) \\ \{\phi(y) : y \in B \wedge y \in x\} & \text{otherwise} \end{cases} \tag{7}$$

satisfies, *for extensional* $B$,

$$\vdash_{\mathfrak{T}'} x \in B \wedge y \in B \rightarrow \big(x \in y \leftrightarrow \phi(x) \in \phi(y)\big) \tag{8}$$

$$\vdash_{\mathfrak{T}'} \phi \text{ is 1-1} \tag{9}$$

[†] $\phi(x) = C(B, x)$ in the notation of VI.2.36. $N$ and $f$ are fixed points of $\phi$. (Why?)

and

$$\vdash_{\mathfrak{T}'} \operatorname{ran}(\phi) \text{ is transitive}^{\dagger} \tag{10}$$

By the first case of (7)

$$\vdash_{\mathfrak{T}'} x \in B \to \big(U(x) \leftrightarrow U(\phi(x))\big) \tag{11}$$

where $\mathfrak{T}'$ is the conservative extension of $\mathfrak{T}$ obtained by adding the introducing axiom for $\phi$.[‡] Its language is $L''$, that is, $L'$ with $\phi$ added.

Now, $\mathfrak{I}' = (L'', \mathfrak{T}', B)$ is also a model of $\mathrm{ZF} + (\mathbb{V} = \mathbb{L})$, and (8)–(11) yield a formal isomorphism (cf. p. 84) between $\mathfrak{I}'$ and the *transitive* interpretation of $L$, $\mathfrak{J} = (L'', \mathfrak{T}', \operatorname{ran}(\phi))$.[§] In fact $\mathfrak{J}$ is a formal $(U, \in)$-*model* of $\mathrm{ZF} + (\mathbb{V} = \mathbb{L})$. To see this we employ I.7.12 to obtain

$$\vdash_{\mathfrak{T}'} \mathscr{A}^{B} \leftrightarrow \mathscr{A}^{\operatorname{ran}(\phi)} \tag{12}$$

for all sentences over $L$. This and (4) entail

$$\vdash_{\mathfrak{T}'} \mathscr{A} \leftrightarrow \mathscr{A}^{\operatorname{ran}(\phi)} \tag{13}$$

for all $L$-sentences. If now $\mathscr{F}$ is the universal closure of a $\mathrm{ZF} + (\mathbb{V} = \mathbb{L})$ axiom, then $\vdash_{\mathfrak{T}'} \mathscr{F}$; hence, by (13), we also have $\vdash_{\mathfrak{T}'} \mathscr{F}^{\operatorname{ran}(\phi)}$.

We note two more facts:

$$\vdash_{\mathfrak{T}'} \operatorname{Card}(\operatorname{ran}(\phi)) \overset{\text{by (9)}}{=} \operatorname{Card}(B) \leq \mathfrak{m} \tag{14}$$

$$\vdash_{\mathfrak{T}'} \{N\} \cup N \cup A \subseteq \operatorname{ran}(\phi) \tag{15}$$

the latter by Exercise VI.6, since $\{N\} \cup N \cup A$ is transitive. By (15) and results in Sections VI.8 and VI.9, $\alpha \mapsto F_\alpha$ is absolute for $\operatorname{ran}(\phi)$ (i.e., for $\mathfrak{J}$); hence so is ord, since it is introduced by the explicit definition[¶]

$$\operatorname{ord}(x) = \min\{\alpha : x = F_\alpha\}$$

Then

$$\vdash_{\mathfrak{T}'} x \in A \to \operatorname{ord}(x) \in \operatorname{ran}(\phi) \qquad \text{(using (15))}$$

Hence, by transitivity of $\operatorname{ran}(\phi)$,

$$\vdash_{\mathfrak{T}'} x \in A \to \operatorname{ord}(x) \subseteq \operatorname{ran}(\phi)$$

[†] This does not need the extensional nature of $B$. By the way, $\vdash_{\mathfrak{T}'} \operatorname{ran}(\phi) = C(B, B)$ in the notation of VI.2.38.

[‡] Extensions by definitions are conservative. Cf. I.6

[§] Where $U$, $\in$, $N$ and $f$ are interpreted as themselves, just as in $\mathfrak{I}'$. cf. footnote to the definition of $\phi$.

[¶] $\operatorname{ord}(x) = \alpha \leftrightarrow (x = F_\alpha \wedge (\forall \beta \in \alpha) x \neq F_\beta)$, etc.

Further, bringing (14) in,

$$\vdash_{\mathfrak{T}'} x \in A \to \text{Card}(\text{ord}(x)) \leq \mathfrak{m} \tag{16}$$

Let now $x \in A$. Suppose also $\mathfrak{m}^+ \leq \text{ord}(x)$. Thus ($\leq$ is $\subseteq$), $\mathfrak{m}^+ \leq \text{Card}(\text{ord}(x))$, contradicting (16). Hence $\text{ord}(x) < \mathfrak{m}^+$, and therefore $x \in \{F_\beta : \beta < \mathfrak{m}^+\}$. We have shown

$$\vdash_{\mathfrak{T}'} A \subseteq \{F_\beta : \beta < \mathfrak{m}^+\}$$

Invoking the deduction theorem and remembering the assumptions (1) (with frozen variables) that we made at the beginning of the proof, we have a proof in $\mathfrak{T}'$ of "if $A$ is a transitive set, $\mathfrak{m}$ an infinite cardinal, and $\text{Card}(A) \leq \mathfrak{m}$, then $A \subseteq \{F_\beta : \beta < \mathfrak{m}^+\}$". This is precisely the statement of the lemma, and we are done, for this *argot* can be trivially translated into a formula over $L$. The conservatism of $\mathfrak{T}'$ means that we have proved the quoted statement in $\text{ZF} + (\mathbb{V} = \mathbb{L})$. □

## VII.8. Exercises

**VII.1.** Show that $\omega \sim \omega + 2$.

**VII.2.** Show that if $A \sim B$, then $A$ is finite iff $B$ is finite.

**VII.3.** Fill in the missing details in the proof of Proposition VII.1.19.

**VII.4.** Show that the concatenation of any finite number of $(\mathscr{I}, \mathscr{F})$-derivations is a $(\mathscr{I}, \mathscr{F})$-derivation.

**VII.5.** Prove, using first Definition VII.1.32 and then Definition VII.1.3, that for any $x$ and $y$ such that $x \neq y$, both $\{x\}$ and $\{x, y\}$ are finite. Use the second method to also compute their cardinality.

**VII.6.** Fill in any missing details in the proof of Proposition VII.1.35.

**VII.7.** Show, using induction on WR-finite sets, that if $A$ is WR-finite and $f$ is a function, then $f[A]$ is WR-finite.

**VII.8.** Show that every natural number is WR-finite.
(*Hint.* Induction on WR-finite sets.)

**VII.9.** Prove that if $A$ is WR-finite and $B \subseteq A$, then $B$ is WR-finite. (Do not use the equivalence of finite with WR-finite.)

**VII.10.** Prove, by induction on finite sets, that if $A$ is finite and $<$ is a partial order on $A$, then $A$ has both a $<$-minimal and a $<$-maximal element.

**VII.11.** Using the previous problem, give an alternative proof that $\omega$ is infinite.
(*Hint.* Consider the partial order $\in$ on $\omega$.)

**VII.12.** If $|A| = n + 1$ and $a \in A$, then $|A - \{a\}| = n$.

**VII.13.** If $A$ and $B$ are finite, then so are $A \cap B$, $A \cup B$, $A - B$, and $A \times B$. (*Hint.* It is convenient to use induction on finite sets for the cases "$\cup$" and "$\times$".)

**VII.14.** If $A$ is finite, then $\mathbf{P}(A)$ is finite. In fact, show that if $|A| = n$, then $|\mathbf{P}(A)| = 2^n$.

(*Hint.* Use induction on $n$. Alternatively, count the subsets of $A$ by counting their *characteristic functions*.[†])

**VII.15.** Show that if $A$ is an infinite set and $B$ is finite, then $A \cup B$, $A \times B$, and $A - B$ are also infinite, whereas $A \cap B$ is finite.

**VII.16.** Show that if $A$ is enumerable and $B$ is finite, then $A \cup B$ and $A - B$ are also enumerable.

**VII.17.** Show that a set is finite iff all its proper subsets are finite.

**VII.18.** Without using the notion of WR-finite, show that for any finite set $A$ and any function $f$, $f[A]$ is finite.

**VII.19.** Show that the set of finite subsets of $\omega$ is enumerable.

(*Hint.* Identify these sets with their characteristic functions.)

**VII.20.** Show that the function $f$, defined in the proof of Theorem VII.2.5, is strictly increasing.

**VII.21.** Give a proof of Corollary VII.2.6 without the help of V.3.9 – in particular, without the help of the axiom of choice.

**VII.22.** Show that if $A$ is countable and $f : A \to B$ is onto, then $B$ is countable.

**VII.23.** Show that the enumeration pictured in Example VII.2.17 (p. 448) is given by the function $f^{-1}$, where

$$f = \lambda xy.\frac{(x+y)(x+y+1)}{2} + y$$

Also show that $f$ is a 1-1 correspondence $\omega^2 \sim \omega$.

**VII.24.** Show that $\lambda xy.2^x(2y+1) - 1$ provides a 1-1 correspondence $\omega^2 \sim \omega$. (*Hint.* Relate this to the prime factorization theorem, and observe that all primes except 2 are odd.)

**VII.25.** Show that the function $f : \omega^2 \to \omega$ given by $f(x, y) = (x + y)^2 + y$ is 1-1 but not onto.

(*Hint.* For "not onto" find an example. For 1-1, find a $g$ such that $g \circ f = \mathbf{1}$ (see Proposition V.3.4). Finding $g : \omega \to \omega^2$ amounts to

[†] If $A \subseteq X$ and the set $X$ is fixed throughout the discussion, then the characteristic function of $A$ (with respect to $X$ being understood) is the function $\chi_A = \lambda x.\mathbf{if}\ x \in A\ \mathbf{then}\ 0\ \mathbf{else}\ 1$.

solving the equation $z = (x + y)^2 + y$ for (unique, of course) $x$ and $y$ in $\omega$. Why?)

**VII.26.** Fill in the missing details in the argument of Example VII.2.20.

**VII.27.** An *algebraic* number is a real root of a polynomial with integer coefficients. For example, $\sqrt{2}$ is algebraic (root of $x^2 - 2 = 0$). Each $n \in \mathbb{Z}$ is algebraic. It is known that the number $\pi$ is not algebraic. (Non-algebraic numbers are called *transcendental*.) Show that the set of all algebraic numbers is enumerable.
(*Hint.* Use the fact that a polynomial of degree $n$ can have at most $n$ real roots.)

**VII.28.** Prove Theorem VII.2.25 only with the aid of Lemma VII.2.23.
(*Hint.* If $A$ is infinite, then it has an enumerable subset $B$, by Lemma VII.2.23. Let $b \in B$. Then $B - \{b\}$ is a proper enumerable subset of $B$, by Exercise VII.16.)

**VII.29.** Without the help of the axiom of choice, show that the set of irrational numbers, $\mathbb{R} - \mathbb{Q}$, is equipotent with $\mathbb{R}$.
(*Hint.* Find, in $\mathbb{R} - \mathbb{Q}$, a set of irrational numbers equinumerous with $\mathbb{Q}$.)

**VII.30.** Prove Corollary VII.3.3.
(*Hint.* This follows from the technique of Example VII.3.1. Define $d$ so that it is a member of ${}^{\omega}2$.)

**VII.31.** Fill in the missing details in Example VII.3.5.

**VII.32.** Show that every number in $[0, 1]$ with a finite binary expansion is rational.

**VII.33.** Show that every non-zero number in $[0, 1]$ has an infinite binary expansion.
(*Hint.* If it has a finite expansion, show that it also has an infinite expansion.)

**VII.34.** Show that for any reals $a < b$, $(a, b) \sim (a, b] \sim [a, b) \sim [a, b] \sim \mathbb{R}$.

**VII.35.** Show that $(0, 1] \times (0, 1] \sim (0, 1]$, *without the help of Cantor-Bernstein theorem*, as follows: Identify each real in $(0, 1]$ with its unique *infinite* decimal expansion. At first, experiment as follows: Given $.a_0a_1a_2 \ldots a_i \ldots \in (0, 1]$, form the pair $\langle .a_0a_2 \ldots a_{2i} \ldots, .a_1a_3 \ldots a_{2i+1} \ldots \rangle$. For example, $.140567\ldots$ yields $\langle .106\ldots, .457\ldots \rangle$, and

$$.5510\underbrace{10\ldots}_{\text{all 10's}} \text{ yields } \langle .51\underbrace{1\ldots}_{\text{all 1's}}, .50\underbrace{0\ldots}_{\text{all 0's}} \rangle.$$

This last example shows that our tentative plan needs an amendment, for the second component of the pair is not a “real” as we understand them in this problem. Make an appropriate amendment to obtain a 1-1 correspondence.

(*Hint.* Revise the way you split $.a_0a_1a_2\ldots a_i\ldots$ into the blocks that you use to alternately build the two components of the pair, so that each block contains a non-zero digit.)

**VII.36.** Show, using the previous problem, that $\mathbb{R}^2 \sim \mathbb{R}$.

**VII.37.** Prove Proposition VII.4.11.

**VII.38.** Show that $\alpha \mapsto \aleph_\alpha$ is onto $\mathrm{Cn} - \omega$.

**VII.39.** Show that if $a \sim a'$ and $b \sim b'$, then $a \preccurlyeq b$ yields $a' \preccurlyeq b'$, and $a \prec b$ yields $a' \prec b'$.

**VII.40.** (Tarski.) Show *without* the help of AC that a set $x$ is infinite iff $\mathbf{P}(\mathbf{P}(x))$ contains an enumerable subset.

(*Hint.* Consider the function $f : \omega \to \mathbf{P}(\mathbf{P}(x))$ given by $f(n) = \{a \in \mathbf{P}(x) : a \sim n\}$.)

**VII.41.** For any $\alpha, \beta$, show that $\mathrm{Card}(\alpha + \beta) = \mathrm{Card}(\alpha) +_c \mathrm{Card}(\beta)$.

**VII.42.** Show that $\mathfrak{a} < \mathfrak{b}$ does *not*, in general, imply $\mathfrak{a} +_c \mathfrak{c} < \mathfrak{b} +_c \mathfrak{c}$.

**VII.43.** Without using VII.5.14, prove that $\mathfrak{a} +_c c = c$ for all $\mathfrak{a} \le c$, where $c = \mathrm{Card}(\mathbb{R})$.

**VII.44.** Prove VII.5.12 in a different way: Use induction on $n$.

**VII.45.** For any $\alpha, \beta$, show that $\mathrm{Card}(\alpha \cdot \beta) = \mathrm{Card}(\alpha) \cdot_c \mathrm{Card}(\beta)$.

**VII.46.** Show that for all $\alpha, \beta$, $\aleph_\alpha +_c \aleph_\beta = \aleph_\alpha \cdot_c \aleph_\beta = \aleph_{\alpha\cup\beta}$.

**VII.47.** Show that for all $\mathfrak{a} > 0$, $0^{\mathfrak{a}} = 0$.

**VII.48.** Show that $(\mathfrak{a} \cdot_c \mathfrak{b})^{\mathfrak{c}} = \mathfrak{a}^{\mathfrak{c}} \cdot_c \mathfrak{b}^{\mathfrak{c}}$ for all $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$.

**VII.49.** Fill in all the missing details in the proof of VII.5.21.

**VII.50.** Compute $n^{\aleph_0}$ for all $n \in \omega$.

**VII.51.** Compute $c^{\aleph_0}$.

**VII.52.** Show that $c < c^c$.

**VII.53.** Compute $(c^c)^c$ in terms of $\mathfrak{f} = \mathrm{Card}({}^{\mathbb{R}}\mathbb{R})$.

**VII.54.** Compute the cardinality of the set of all *continuous* real-valued functions on $\mathbb{R}$.

(*Hint.* A continuous function is uniquely determined by its restriction on $\mathbb{Q}$, the set of rational numbers.)

**VII.55.** Compute the cardinality of the set of all *differentiable* real-valued functions on $\mathbb{R}$.

**VII.56.** Show that $\aleph_\alpha^{\aleph_\beta} = 2^{\aleph_\beta}$ on the assumption that $\alpha \leq \beta$.

(*Hint.* Use VII.5.21 and VII.4.25.)

**VII.57.** Show that if $\mathfrak{k} \leq \mathfrak{l}$, then $\mathfrak{a}^{\mathfrak{k}} \leq \mathfrak{a}^{\mathfrak{l}}$.

**VII.58.** Prove that for any ordinal $\alpha$, $\mathrm{cf}(\aleph_{\alpha+\omega}) = \omega$.

**VII.59.** Prove that if $A_i \sim B_i$ for all $i \in I$, and if $A_i \cap A_j = \emptyset = B_i \cap B_j$ whenever $i \neq j$, then $\bigcup_{i\in I} A_i \sim \bigcup_{i\in I} B_i$.

**VII.60.** Prove that $\mathrm{Card}(\bigcup_{i\in I} A_i) \leq \sum_{i\in I} \mathrm{Card}(A_i)$.

**VII.61.** Prove that $\mathfrak{a}_i \leq \mathfrak{b}_i$ for all $i \in I$ implies $\sum_{i\in I} \mathfrak{a}_i \leq \sum_{i\in I} \mathfrak{b}_i$.

**VII.62.** Prove that $\sum_{i\in\mathfrak{m}} \mathfrak{k}_i = \mathfrak{m} \cdot_c \sup_{i\in\mathfrak{m}} \mathfrak{k}_i$, if $\mathfrak{k}_i > 0$ for all $i$, and at least one cardinal among $\mathfrak{m}$ and $\mathfrak{k}_i$ is infinite.

**VII.63.** Prove that an infinite cardinal $\mathfrak{a}$ is singular iff there are cardinals $\mathfrak{b} < \mathfrak{a}$ and $\mathfrak{m}_\lambda < \mathfrak{a}$, for all $\lambda < \mathfrak{b}$, such that $\mathfrak{a} = \sum_{\lambda\in\mathfrak{b}} \mathfrak{m}_\lambda$.

**VII.64.** If $A_i \sim B_i$ for $i \in I$, then $\prod_{i\in I} A_i \sim \prod_{i\in I} B_i$.

**VII.65.** Show that $\mathrm{cf}(2^{\aleph_\alpha}) > \aleph_\alpha$ for any $\alpha$.

**VII.66.** (Bernstein.) Prove that $\aleph_n^{\aleph_\alpha} = 2^{\aleph_\alpha} \cdot_c \aleph_n$ for all $n \in \omega$ and all $\alpha$.

**VII.67.** Define the *beth* function, $\beth$, by the induction $\beth_0 = \aleph_0$, $\beth_{\alpha+1} = 2^{\beth_\alpha}$ and, if $\mathrm{Lim}(\alpha)$, $\beth_\alpha = \bigcup_{\beta<\alpha} \beth_\beta$. Show that $\beth$ has fixpoints.

**VII.68.** Show that if GCH holds, then $\beth_\alpha = \aleph_\alpha$ for all $\alpha$.

**VII.69.** Let $\mathrm{Card}(N) < \omega$. Show that $\mathrm{Card}(V_N(\omega + \alpha)) = \beth_\alpha$ for all $\alpha$.

**VII.70.** Show that if $\mathrm{Lim}(\alpha)$, then $V_N(\alpha)$ is a model of ZFC less collection.

**VII.71.** Let $\mathrm{Card}(N) < \alpha$, where $\alpha$ is strongly inaccessible. Then the following are absolute for $V_N(\alpha)$:

(1) $\beta$ is a cardinal,
(2) $f : \beta \to \gamma$ is cofinal,
(3) $\mathrm{cf}(\beta)$,
(4) $\beta$ is strongly inaccessible.

**VII.72.** Prove that "$\beta$ is a cardinal" is not absolute for $V_N(\omega + 2)$.

**VII.73.** Let $R$ be a relation on a set $A$. Define $Wf(R)$, the *well-founded part* of $R$, as the set $\{a \in A :$ there is *no* infinite chain $\ldots R\ a_2 R\ a_1\ R\ a\}$ (where, of course, all the $a_i$ are in $A$, since $R \subseteq A \times A$). Prove that $\mathrm{Cl}(\widetilde{R}) = Wf(R)$, where $\widetilde{R}$ on $\mathbf{P}(A) \times A$ is given by

$$X \overset{\widetilde{R}}{\mapsto} x \quad \text{iff} \quad X = R\langle x\rangle$$

(*Hint.* For $\subseteq$ use induction on the structure of $\text{Cl}(\widetilde{R})$. For $\supseteq$ recall VI.2.13 and use MC over $Wf(R)$.)

**VII.74.** Prove that the rule set that defines the syntax of the formulas of propositional calculus is unambiguous. This rule set, $P$, is

$$\begin{aligned} \emptyset &\mapsto p \qquad \text{for each variable } p \\ \{x, y\} &\mapsto (x \vee y) \\ \{x, y\} &\mapsto (y \vee x) \\ \{x\} &\mapsto (\neg x) \end{aligned}$$

(*Hint.* Show by induction over $\text{Cl}(P)$ that (1) every member of $\text{Cl}(P)$ has as many "("-symbols as ")"-symbols, (2) every nonempty proper (string) prefix of a member of $\text{Cl}(P)$ has strictly more "("-symbols than ")"-symbols. The rest should be easy.)

**VII.75.** Prove that the rule set that defines the syntax of the *fully parenthesized* arithmetic expressions (on the symbol set $\{1, 2, 3, \times, +, (, )\}$) is unambiguous. This rule set, $P$, is

$$\begin{aligned} \emptyset &\mapsto p \qquad \text{for } p = 1, 2, 3 \\ \{x, y\} &\mapsto (x + y) \\ \{x, y\} &\mapsto (y + x) \\ \{x, y\} &\mapsto (x \times y) \\ \{x, y\} &\mapsto (y \times x) \end{aligned}$$

(*Hint.* As in the preceding exercise.)

**VII.76.** Imitate Exercise VII.75 to define a rule set that defines all the *terms* of a first order language, and prove that your rule set is unambiguous.

**VII.77.** Imitate Exercise VII.75 to define a rule set that defines all the formulas of set theory, and prove that this rule set is unambiguous
(*Hint.* Brackets, once again, are important.)

**VII.78.** Prove that for any total operator $\Gamma$ (even one that is a proper class), $\Gamma^\alpha$ is a set for all $\alpha$.

**VII.79.** Prove VII.6.31 differently: Invoke Gödel's second incompleteness theorem.

# VIII

# Forcing

The method of forcing was invented by Cohen (1963) towards the construction of non-standard models of ZFC, so that "new axioms" could be proved consistent with the standard ones. Our retelling of the basics of forcing found in this chapter is indebted primarily to the user-friendly account found in Shoenfield (1971). The influence of the expositions in Burgess (1978), Jech (1978b), and Kunen (1980) should also be evident.

In outline, the method goes like this: Suppose we want to show that ZFC (sometimes ZF or an even weaker subtheory) is consistent with some weird new axiom, "NA". Working in the metatheory, one starts with a CTM, $M$,[†] for ZFC. This is the *ground model*. One then judiciously chooses a PO set,[‡] $\langle P, <, 1\rangle$, *in* $M$ – where we find it convenient to restrict attention to PO sets that have a maximum element (let us call the latter "1") – and, using the PO set, one constructs a so-called *generic* set $G$. Circumstances normally have $G$ obey $G \notin M$. The "judicious" aspect of the choice of the PO set will entail that the *generic extension*, $M[G]$, of the CTM $M$ not only contains $G$ as an element but is a CTM itself that satisfies NA as well (i.e., $\models_{M[G]} \text{ZFC} + \text{NA}$). Thus, one has a proof *in the metatheory* that if ZFC is consistent (i.e., if a CTM for ZFC exists), then so is ZFC + NA.

We have said above that "$\langle P, <, 1\rangle \in M$". By absoluteness of pair (see Section VI.8), the quoted statement is equivalent to "$P \in M$ and $< \in M$ and $1 \in M$".

[†] We know that we have used the symbol $M$ for $\{x : U(x)\}$. However, it is normal practice for people to also denote by $M$ an arbitrary CTM of ZFC. We are rapidly running out of symbols; therefore we ask the reader to allow us this overloading of the letter $M$ with more meanings than one. As always, we will invoke context in our defense.

[‡] This is the hard part of the method.

The above argument cannot be formalized in ZFC "as is" to provide a finitary proof of relative consistency, namely, along the lines "if ZFC is consistent, here is how we can *construct a set model* for ZFC + NA *in ZFC*". Unfortunately such a construction would formally prove as a corollary (in ZFC) that ZFC is itself consistent, clashing with Gödel's second incompleteness theorem.

**Pause.** In ZF we have shown how to construct a model, $\mathbb{L}$, of ZFC + GCH. Why does this not contradict Gödel's second incompleteness theorem?

We can still circumvent this difficulty and provide finitary proofs of relative consistency results of the type "if ZFC is consistent, then ZFC + NA is too", using forcing. One attempts the contrapositive instead:

$$\text{If} \quad \vdash_{\text{ZFC+NA}} 0 \neq 0, \quad \text{then} \quad \vdash_{\text{ZFC}} 0 \neq 0 \tag{1}$$

But the if part means that for some *finite set* of axioms of ZFC, $\Gamma$,

$$\Gamma \cup \{\text{NA}\} \vdash 0 \neq 0 \tag{2}$$

Now, we can construct a CTM, $M$, *just for* $\Gamma$, *inside* ZFC using reflection (cf. VII.7.23 and the proof of VII.7.24) followed by Mostowski collapsing. Using forcing, and continuing to work formally inside ZFC, we get a generic extension of $M$, $M[G]$, that is a formal model of $\Gamma \cup \{\text{NA}\}$. Now this is fine by Gödel's second theorem, for $\Gamma$ is *not* the entire ZFC axiom set. By (2), we have shown $\vdash_{\text{ZFC}} (0 \neq 0)^{M[G]}$, and hence $\vdash_{\text{ZFC}} 0 \neq 0$, since 0 is absolute for transitive classes. This concludes the forcing proof of (1) in a finitary manner.

*We will do our forcing arguments in the metatheory.*

**A Note on Proofs.** We will be working in the metatheory throughout most of this chapter, using the ZF axioms as our hypotheses (sometimes adding AC). We will do so usually from within $\mathbb{U}_A$ (for a usually unspecified set of start-up atoms, $A$), but often from within some CTM $M$, that is, relativizing formulas and arguments to $M$.

Our proof terminology will be similar to that of the "practising mathematician". We will say "true" or "false" for sentences (whereas before we have always said "provable" or "refutable") and, moreover, we will usually refrain from reminding the reader that this or that principle of logic (e.g., proof by auxiliary constant, deduction theorem, proof by cases, etc.) is at work.

## VIII.1. PO Sets, Filters, and Generic Sets

In this chapter we will fix attention on special types of PO sets that have a maximum element (which is, of course, unique), invariably denoted by "1".

**VIII.1.1 Definition.** Let $\langle P, <, 1\rangle$ be a PO set with a maximum element – which we will denote by "1". Throughout this chapter we will call the members of $P$ *forcing conditions* or just *conditions*, and such PO sets *notions of forcing*. We will use the letters $p, q, r, s$, with or without primes or subscripts, for conditions.

If $p = q \vee p < q$, we write $p \leq q$ and say that $p$ *extends*, or *is an extension of*, $q$.[†] When $p < q$, then $p$ is a *proper extension* of $q$. Two conditions $p$ and $q$ are *compatible* iff there is an $r \in P$ such that $r \leq p$ *and* $r \leq q$. If two conditions $p$ and $q$ are *not* compatible, then they are *incompatible* and we write $p \perp q$.

The abbreviation "$p$ and $q$ are *comparable*" stands for "$p = q \vee p < q \vee q < p$".

A set $O \subseteq P$ is *open* iff, for any $p \in O$, $\leq \langle p\rangle \subseteq O$. In particular, every segment $\leq \langle p\rangle$ is open.

A set $D \subseteq P$ is *dense* iff it meets every open set. In other words, for every $p \in P$ there is a $q \in D$ such that $q \leq p$ (i.e., $D \cap \leq \langle p\rangle \neq \emptyset$).

A *chain* over the PO set[‡] $P$ is a set $C \subseteq P$ such that any two elements of $C$ are comparable.

An *antichain* over the PO set $P$ is a set $A \subseteq P$ such that every two of its members are incompatible. □

**VIII.1.2 Remark.** In structure parlance (cf. Section I.5) a PO set $\langle P, <, 1\rangle$ is a *structure*, with underlying set (or *domain*) $P$ and with $<$ and 1 as *specified* relation and function (a 0-ary function or constant) respectively. Thus, if need arises, we will use fraktur type (and the same letter as the domain) to name the structure; in the present case, $\mathfrak{P} = \langle P, <, 1\rangle$.

The terms "open" and "dense" are not accidental. There is a strong relation between the homonymous topological concepts and forcing, but this connection with topology will not be pursued here. By the way, the fully qualified terms are $\mathfrak{P}$-open and $\mathfrak{P}$-dense respectively, but usually the qualification is omitted and $\mathfrak{P}$ is understood from the context. □

[†] Yes, the extension is the "smaller" of the two. This terminology is due to Cohen (1963).

[‡] Recall that when the order $<$ is understood, we say "PO set $P$" instead of "PO set $\langle P, <, 1\rangle$".

**VIII.1.3 Example.** The set of finite functions from $\omega$ to $\{0, 1\}$, i.e.,

$$\{f : f \text{ is a function and } \operatorname{dom}(f) \in \omega \wedge \operatorname{ran}(f) \subseteq 2\} \tag{1}$$

can be given a PO set structure as follows: Define $f < g$ to mean $g \subset f$ (we order by "reverse inclusion"). Here $\emptyset : \omega \to 2$ is 1, the maximum element. For the sake of future reference, let us give this PO set the name $\mathfrak{O} = \langle O, <, 1\rangle$ (or $\mathfrak{O} = \langle O, \supset, \emptyset\rangle$), where we have used the name "$O$" for the set displayed in (1). We also note that $\mathfrak{O}$ has no minimal elements. Such an element would be a finite function that had no finite proper extension. □

**VIII.1.4 Definition.** Let $\langle P, <, 1\rangle$ be a PO set as in VIII.1.1.

A set $F \subseteq P$ is a *filter over* $\langle P, <, 1\rangle$ – also called a $\langle P, <, 1\rangle$-filter, or a $P$-filter if $<$ is understood, or just a filter if $P$ is also understood – provided the following conditions are fulfilled:

(1) $1 \in F$.
(2) For any two members $p$ and $q$ of $F$ there is an $r$ in $F$ such that $r \leq p$ and $r \leq q$.
(3) If $p \in F$ and $p \leq q$, then $q \in F$ (or, $p \in F \to {\geq}\langle p\rangle \subseteq F$). □

In view of (3) in VIII.1.4, (1) is equivalent to the requirement "$F \neq \emptyset$".

Note that in (2) we have asked more than compatibility of any two members of $F$: We want this compatibility to be "witnessed" inside $F$.

In algebra people define their filters in a stronger manner. First off, one requires that the PO set $\mathfrak{P}$ be a *lattice*, that is, for any two of its members $p$ and $q$, both $\sup\{p, q\}$ and $\inf\{p, q\}$ exist.[†] One then calls an $F \subseteq P$ a filter if it satisfies

(i) $F \neq \emptyset$ (same as (1) in VIII.1.4 if the lattice has a maximum element),
(ii) for any two members $p$ and $q$ of $P$, $\inf\{p, q\} \in F$ iff $\{p, q\} \subseteq F$.

Note that if $F$ is a filter in the sense (i)–(ii) over the lattice $\mathfrak{P} = \langle P, <, 1\rangle$, then it is as well in the sense (1)–(3) of VIII.1.4 over the PO set $\mathfrak{P}$. Indeed, by (ii), if $p$ and $q$ are in $F$, then so is $\inf\{p, q\}$, providing the "witness" that (2) requires. Also, if $p \in F$ and $p \leq q$ ($q \in P$), then $p = \inf\{p, q\}$; hence (by (ii)) $q \in F$.

[†] sup and inf were defined in VI.5.23.

**VIII.1.5 Example.** Fix a PO set $\mathfrak{P}$. The set $\{1\}$ is a filter.

If $\emptyset \neq S \subseteq P$ is a chain, then we can build the $\subseteq$-smallest filter that contains $S$. We call it the *filter generated by* $S$.

To see that this exists, define

$$F \stackrel{\text{def}}{=} \{p \in P : (\exists q \in S) q \leq p\} \tag{$*$}$$

Trivially (by $x \leq x$), $S \subseteq F$. We next verify that $F$ is a filter. For property (1) (of VIII.1.4), pick any $q \in S$ ($S$ is not empty). But then $q \leq 1$; hence $1 \in F$ by $(*)$. Property (3) is also trivially verified. As for (2), let $p$ and $p'$ be in $F$. Then $q \leq p$ and $q' \leq p'$ for some $q$ and $q'$ in $S$. For the sake of concreteness, say $q \leq q'$ (by comparability of $S$-elements). Then $q$ is an appropriate witness for the compatibility of $p$ and $p'$.

Let $F'$ be any filter such that

$$S \subseteq F' \tag{$**$}$$

Let $p \in F$ and also $q$ (in $S$, by $(*)$) such that $q \leq p$. Since $q \in F'$ by $(**)$ and $F'$ is a filter, it follows that $p \in F'$. Thus, $F \subseteq F'$. □

**VIII.1.6 Example.** Refer to the PO set $\mathfrak{O}$ of VIII.1.3. Suppose that $F$ is a filter over $\mathfrak{O}$. Then $\bigcup F$ is single-valued (by VIII.1.4(2)), i.e., a function $\omega \rightarrow 2$. □

**VIII.1.7 Definition (Generic Sets).** Given a PO set $\mathfrak{P} = \langle P, <, 1\rangle$ and a set $M$. A subset $G \subseteq P$ is called *$M$-generic* iff

(1) $G$ is a filter over $\mathfrak{P}$,
(2) $G$ meets every $P$-dense set $D$ that is a member of $M$ (that is $G \cap D \neq \emptyset$). □

The reader is reminded that the phrase "$D$ is $P$-dense" subsumes the subphrase "$D \subseteq P$"; see VIII.1.1 and VIII.1.2.

**VIII.1.8 Theorem (Generic Existence Theorem).** *Let $\mathfrak{P} = \langle P, <, 1\rangle$ be a notion of forcing, and $M$ be countable. Fix any $p \in P$. Then there is an $M$-generic set $G \subseteq P$ such that $p \in G$.*

*Proof.* Let $m_0, m_1, m_3, \ldots$ be a fixed enumeration of $M$. We define by recursion a function $f$ on $\omega$ by

$$f(0) = p$$

and

$$f(n+1) = \begin{cases} m_{\text{smallest } k \text{ such that } m_k \in \leq \langle f(n)\rangle \cap m_n} & \text{if } \leq \langle f(n)\rangle \cap m_n \neq \emptyset \\ f(n) & \text{if } \leq \langle f(n)\rangle \cap m_n = \emptyset \end{cases} \qquad (*)$$

Note that the explicit definition of the subscript "$k$" above avoids an infinite set of "unspecified choices" (AC). Also note that the last case above always obtains if $m_n$ is an urelement.

It is easy to see that $\text{ran}(f)$ is a nonempty ($p \in \text{ran}(f)$) chain: First off, that $\text{ran}(f) \subseteq P$ is trivial. Next, the reader can verify that $(\forall n \in \omega) f(n+1) \leq f(n)$ holds (induction on $n$; the last case in the definition of $f$ guarantees that $f$ is total on $\omega$).

Taking for $G$ the filter generated by the chain $\text{ran}(f)$ (see VIII.1.5) will do. Indeed, that $p \in G$ is trivial. Let then $D \in M$ be dense. Now $D = m_n$ for some $n$. Then the first condition in $(*)$ gives us $f(n+1) = m_k$, where $m_k \in \leq \langle f(n)\rangle \cap D$. Since $m_k \in G$, we have $G \cap D \neq \emptyset$. □

**VIII.1.9 Example.** Let $M$ be a CTM for, say, ZF. We will consider the PO set of VIII.1.3 relativized in $M$. By absoluteness of pairing and finiteness (see Section VI.8), $\{a, b\}$, ordered pairs, and finite functions are ($M$-) absolute, and so is $\mathbf{P}_\omega(A)$ defined as $\{x : x \subseteq A \wedge x \text{ is finite}\}$ (see Exercise VIII.3). We also recall that finite ordinals (and $\omega$), dom, and ran are absolute for $M$.

Thus one may redo Example VIII.1.3, this time arguing from within $M$, as an inhabitant[†] of $M$ would do, to obtain *in M* the PO set $\mathfrak{P} = \langle P, \supset, \emptyset\rangle$, where

$$P = \{p : p \text{ is a function } \wedge \text{dom}(p) \in \omega \wedge \text{ran}(p) \subseteq 2\} \qquad (1)$$

He will conduct his argument by noting that $\omega$ and 2 are in $M$, and therefore so is $\omega \times 2$; thus $P \in M$, by separation, since[‡] $P = \{p \in \mathbf{P}_\omega(\omega \times 2) : p \text{ is a function} \wedge \text{dom}(p) \in \omega\}$ (he knows that $M$ is a ZF model, so he can do all that). It then follows that $\mathfrak{P}$ is in $M$ as well, by the fact that $M$ is closed under pairing.

**Pause.** Why doesn't he just say that $P$ is a set by separation, since $P \subseteq M$?

Equivalently, a being of $\mathbb{U}_A$ argues the same thing by making the case that $P^M$ given in

$$P^M = \{p \in \mathbf{P}_\omega(\omega \times 2) : p \text{ is a function } \wedge \text{dom}(p) \in \omega\} \qquad (1')$$

[†] This person uses just "$\{p$ : etc.$\}$" rather than "$\{p \in M$ : etc.$\}$", since the $\in M$ part is implicit; there are no universes beyond $M$ for him.

[‡] For him $\mathbf{P}_\omega(A)$ consists precisely of these finite subsets of $A$ that are also members of $M$ – which are *all* the finite subsets of A, absolutely speaking.

is in $M$, since separation holds in $M$ and $\mathbf{P}_\omega(\omega \times 2) \in M$ (why?). Here we are invoking VI.8.4 and VI.8.13, noting that, *for* $p \in M$, absoluteness makes the presence of a superscript "$^M$" redundant inside the braces in ($1'$) above.

In particular, all this shows that $P$ (hence also $\mathfrak{P}$) is absolute for $M$.

Let $G$ be $M$-generic. Such a $G$ can be constructed by VIII.1.8, since $M$ is countable. Let us continue working in $\mathbb{U}_A$ to construct $G$.

Since $G$ is a filter, $\bigcup G$ is a function (VIII.1.6). Note that, for any $n \in \omega$, the set $D_n = \{p \in P : n \in \mathrm{dom}(p)\}$ is $P$-dense in $M$; for if $q \in P$, then either $q(n) \downarrow$ (in which case $q \in D_n$ – indeed, any extension $p \leq q$ is in $D_n$)[†] or $q(n) \uparrow$. Well, then, define $p = q \cup \{\langle n, 0\rangle\}$ (this is in $M$, by absoluteness of $\cup$ and pairing). We have $p \supset q$ and $p \in D_n$. Thus $G$ meets all the $D_n$, in other words, $n$ is in the domain of $\bigcup G$ for all $n$: $\mathrm{dom}\left(\bigcup F\right) = \omega$.

Is $G \in M$? Suppose yes, and consider the set (in $M$ by absoluteness of difference) $P - G$. This is $P$-dense in $M$: Let $p \in P$. Let $q$ and $r$ be two incompatible extensions of $p$ in $M$. For example, say $n$ is smallest such that $p(n) \uparrow$. Set then $q = p \cup \{\langle n, 0\rangle\}$ and $r = p \cup \{\langle n, 1\rangle\}$. Now $q$ and $r$ cannot both be in $G$ for $q \perp r$. Say $q \notin G$. But then $q \in P - G$. Having established the density of $P - G$ (in $M$), genericity would now imply $(P - G) \cap G \neq \emptyset$, a contradiction.

We have said above "Let us continue working in $\mathbb{U}_A$ to construct $G$". We see that such caution was justified, for an inhabitant of $M$ cannot construct this $G$. □

## VIII.2. Constructing Generic Extensions

Our purpose is to define a procedure which for any CTM $M$ and $M$-generic set $G$ builds a CTM, $M[G]$, that is the $\subseteq$-smallest extension of $M$ containing $G$ as a member. Such an extension is called a *generic* or Cohen extension of the *ground model* $M$.

Moreover, we want to be able to empower inhabitants of $M$ to discuss aspects of $M[G]$ notwithstanding the fact that a lot of objects in $M[G]$ are not in $M$ – for example, $G$ under "practical circumstances" is not; see VIII.1.9.

To keep our sanity, we will usually employ the language and methods of ZF (or ZFC, or even of a fragment of ZF) "in the abstract" (i.e., formally) to effect our various constructions.[‡] We can afterwards relativize what we have done

[†] Recall that this $\mathfrak{P}$ has no minimal elements.

[‡] One can view this approach alternatively: We are really working, metamathematically, within the "real" universe, $\mathbb{U}_A$, however restricting our methodology to only employ ZF axioms and rules of logic. Of course, any confirmed Platonist who has followed us this far will say: "That's an odd comment; wasn't it exactly this approach that we took all along?"

to some CTM $M$, using results from Sections VI.8 and, sometimes, VI.9. On occasion, it might be just as easy to work as an inhabitant of $M$ would and, using the methods of ZFC (or ZF, or . . . ), argue in effect from within $M$, as we have done in the initial part of VIII.1.9.

Our discussion will be, in general, dependent upon a PO *set* "variable", which we will invariably call by the nondescript name $\mathfrak{P} = \langle P, <, 1\rangle$. For convenience we will use the (fairly standard) notation

$$|\mathfrak{P}| \text{ stands for } P \tag{1}$$

**VIII.2.1 Definition.** Let $M$ be a set and $\mathfrak{P} \in M$. For any $G \subseteq |\mathfrak{P}|$ we introduce the following abbreviation:

$$a \in_G b \quad \text{stands for} \quad (\exists p \in G)\langle a, p\rangle \in b \tag{1}$$

□

**VIII.2.2 Remark.** We have fixed an $M$ and $\mathfrak{P} \in M$. The relation $x\, \mathbb{P}\, y$ defined by $(\exists G \subseteq |\mathfrak{P}|)x \in_G y$ has MC, as this follows from $x\, \mathbb{P}\, y \to \rho(x) < \rho(y)$, this latter since $x \in \langle x, p\rangle \in y$ for some $p \in G$, for some $G \subseteq |\mathfrak{P}|$[†] (cf. VI.6.24). It is also left-narrow: $x\, \mathbb{P}\, y \to x \in TC(y)$. Thus we can effect recursive definitions with respect to $\mathbb{P}$, and in particular with respect to $\in_G$ (fixed $G$), as well as do $\mathbb{P}$-induction and $\in_G$-induction (fixed $G$). Cf. VI.8.23 and VI.8.24. □

**VIII.2.3 Definition.** Let $M$ be a set, $\mathfrak{P} \in M$, and $G \subseteq |\mathfrak{P}|$. Working in $\mathbb{U}_A$,[‡] we define the *interpretation function*, $\lambda x G.x^G$, by $\mathbb{P}$-recursion:

$$x^G = \begin{cases} x & \text{if } U(x) \\ \{y^G : y \in_G x\} & \text{if } \neg U(x) \end{cases} \tag{1}$$

We will call $a^G$ the *G-interpretation* of $a$. □

More completely, we should add to the definition (1) above, second case, the conjunct "$\wedge\, G \subseteq P \wedge \langle P, <, 1\rangle \in M$ is a PO set".[§] One then adds a third, "otherwise" case where, say, $x^G = \emptyset$. This "completion" spoils the clean form of (1) and adds or subtracts nothing to or from the expected properties of $x^G$

[†] Or $x \in \{x\} \in \langle x, p\rangle \in y$ if one uses the Kuratowski "$\langle \ldots, \ldots \rangle$".

[‡] In ZF in fact, "abstractly" or formally, as we do not use an assumption that $M$ is a CTM.

[§] We mean that $\langle P, <, 1\rangle$ is "really" a PO set, as we carry the definition out in $\mathbb{U}_A$. Anyhow, if $M$ is a CTM, absoluteness of being a PO set would make $\langle P, <, 1\rangle$ a PO set in the eyes of people living in $M$ as well.

used in the sequel. Thus we have stated the missing conditions loosely in the "assumptions" instead.

Note that if we fix $G$, then the above defines $\lambda x.x^G$ by $\in_G$-recursion using $G$ as a "parameter". But whence "interpretation"? This terminology will make sense in the next section.

Finally:

**VIII.2.4 Definition.** Let $M$ be a CTM of ZF, $\mathfrak{P} \in M$, and $G$ an $M$-generic set. We define the set $M[G]$ by

$$M[G] = \{x^G : x \in M\}$$

We call $M[G]$ a *generic extension* or Cohen extension of the *ground model* $M$. □

**VIII.2.5 Remark.** By results and techniques of Section VI.8, $\lambda x G.x^G$ is absolute for transitive models of ZF (see Exercise VIII.4). Thus if $M \subseteq N$ and $N$ is a CTM (of ZF) that satisfies $G \in N$, then

$$N \ni \left(a^G\right)^N = a^G$$

for any $a \in N$, in particular for any $a \in M$. Thus, $M[G] = \{x^G : x \in M\} \subseteq N$. □

We next build tools to show that for any CTM $M$ and $M$-generic $G$, we have $M \subseteq M[G]$ and $G \in M[G]$.

**VIII.2.6 Definition (The Caret).** We define (in ZF formally or in $\mathbb{U}_A$ metamathematically) by $\in$-recursion a function $\lambda x\mathfrak{P}.\hat{x}$:

$$\hat{x} = \begin{cases} x & \text{if } U(x) \\ \{\langle \hat{y}, 1\rangle : y \in x\} & \text{otherwise} \end{cases}$$

where $\mathfrak{P}$ has 1 as the maximum element. □

**VIII.2.7 Remark.** Again, there ought to be a third, "otherwise" case above, yielding, say, $\hat{x} = \emptyset$, whenever the "input" $\mathfrak{P}$ is not as it should be. The present "otherwise" would then become the case "$\neg U(x) \wedge$ ($\mathfrak{P}$ is as it should be)".

Work in Section VI.8 easily yields that the function $\lambda x\mathfrak{P}.\hat{x}$ is absolute (cf. Exercise VIII.5). Thus if $M$ is a CTM of ZF and $\mathfrak{P} \in M$, then $x \in M$ implies that $\hat{x} = (\hat{x})^M \in M$.

In particular, $\big((\lambda x^{\mathfrak{P}}.\hat{x}) \restriction M\big) \in M$. This latter fact can also be seen as follows: A mathematician who lives in $M$ can effect the recursive definition VIII.2.6 in $M$. □

**VIII.2.8 Lemma.** *Let $M$ be a CTM of* ZF*, and $G$ an $M$-generic set with respect to $\mathfrak{P} \in M$. Then $M \subseteq M[G]$ and $G \in M[G]$.*

*Proof.* Let $x \in M$. We do $\in$-induction to prove $(\hat{x})^G = x$; thus $M \subseteq M[G]$, since $\hat{x} \in M$ by VIII.2.7 and therefore $(\hat{x})^G \in M[G]$ (cf. VIII.2.4).

If $U(x)$, then $(\hat{x})^G = x^G = x$.

Let now $\neg U(x)$. Then

$$\begin{aligned}
(\hat{x})^G &= \{y^G : y \in_G \hat{x}\} \qquad \text{by VIII.2.3}\\
&= \{y^G : (\exists p \in G)\langle y, p\rangle \in \hat{x}\}\\
&= \Big\{y^G : \langle y, 1\rangle \in \{\langle \hat{z}, 1\rangle : z \in x\}\Big\} \qquad \text{since } \operatorname{ran}(\hat{x}) = \{1\}\\
&= \{(\hat{z})^G : z \in x\}\\
&= \{z : z \in x\} \qquad \text{by I.H.}\\
&= x
\end{aligned}$$

To prove $G \in M[G]$, we look for an element $\Gamma \in M$ such that $\Gamma^G = G$. We will calculate that

$$\Gamma = \{\langle \hat{p}, p\rangle : p \in P\} \tag{1}$$

will do fine. By closure of $M$ under pairs and by the fact that collection is true in $M$, $\Gamma \in M$. We next calculate

$$\begin{aligned}
\Gamma^G &= \{y^G : (\exists p \in G)\langle y, p\rangle \in \Gamma\}\\
&= \{(\hat{p})^G : p \in G\}\\
&= \{p : p \in G\} \qquad \text{by what we have proved above}\\
&= G
\end{aligned}$$

□

**VIII.2.9 Remark.** $M$ and $M[G]$ have the same urelements. Indeed, $M \subseteq M[G]$ yields that all atoms of $M$ are included in $M[G]$. Conversely, suppose that $U(a^G)$ is true in $M[G]$, and hence in $\mathbb{U}_A$ (recall from Section VI.8 that we set $U^{\mathfrak{M}} = U$ in general in $(U, \in)$-interpretations). From VIII.2.3, $a^G = a$ (otherwise $a^G$ is a set). Thus, $a^G \in M$ (since $a \in M$). □

**VIII.2.10 Example.** $M[G]$ is closed under pairs, that is $z \in M[G] \wedge w \in M[G] \rightarrow \{z, w\} \in M[G]$.

It suffices to find a $u \in M$ such that $u^G = \{z, w\}$. We start by letting $a^G = z$ and $b^G = w$, with $a$ and $b$ in $M$ (VIII.2.4). Since $M$ is a CTM of, say, ZF, its closure under pairing yields $\{\langle a, 1\rangle, \langle b, 1\rangle\} \in M$. Now $u = \{\langle a, 1\rangle, \langle b, 1\rangle\}$ is what we want, for, by VIII.2.3,

$$u^G = \{a^G, b^G\}$$

since $a \in_G u$ and $b \in_G u$. □

**VIII.2.11 Remark.** So far we readily have the "C" and "T" of the expected CTM attributes of $M[G]$. Indeed, by VIII.2.4, the function $\lambda x.x^G : M \to M[G]$ is onto. Since the left field is countable, this settles the "C". As for transitivity, let $x \in y^G \in M[G]$. Then $y^G$ is a set, thus (VIII.2.3) $x = z^G$ for some $z \in_G y$. Therefore, for some $p \in |\mathfrak{P}|$, $z \in \langle z, p\rangle \in y \in M$; hence $z \in M$ by transitivity of $M$. Finally, $x \in M[G]$ by VIII.2.4. □

For the "M", that $M[G]$ is a model of, say, ZFC if $M$ is, we need more work.

## VIII.3. Weak Forcing

Let us fix a CTM $M$ (of ZF, or ZFC, or of some extension, or of a sufficiently strong fragment such as ZF without the power set axiom – the so-called "ZF− P"), as well as a PO set $\mathfrak{P} \in M$. We will be working in the metatheory, within $\mathbb{U}_A$, using those axioms of ZFC for which $M$ is a model. Suppose that we have built $M[G]$ for some $M$-generic $G \subseteq |\mathfrak{P}|$, as in VIII.2.4.

We want to allow inhabitants of $M$ to reason about this $M[G]$. For this purpose they need *names* for the "real objects" of $M[G]$ so that they can write down formulas that can refer to specific objects of $M[G]$, such as $G$.

Now, by VIII.2.4, any object $a \in M[G]$ has the form $b^G$ for some $b \in M$. This $b$, or, formally, a *name for b*, will name $a$.

Thus, we *import* into the basic language of ZFC, $L_{\text{Set}}$, a new constant symbol name for each member of $M$.[†] This is a process familiar to us from I.5.4. However, rather than only using the (*argot*) names $i, j, k$ for members of $M$ – and $\overline{i}, \overline{j}, \overline{k}$ for their formal counterparts in $L_{\text{Set},M}$ – we will continue using any (*argot*) name we please for members of $M$ (such as $a, b, q, p, i, \ldots$) and, as in I.5.4 reserve the *argot* names $\overline{a}, \overline{b}, \overline{p}, \overline{i}, \ldots$ to stand for names of imported constants. Thus, $\overline{a}$ names $a$, etc. $L_{\text{Set},M}$ is called the *forcing language*.

We will now view $M[G]$ as the domain of the structure $\mathfrak{M}_G = (M[G], U, \in)$, and we interpret the language $L_{\text{Set},M}$ in $\mathfrak{M}_G$ in the standard manner (Section I.5).

[†] As we did with $L_{\text{Set}}$, we are free afterwards to extend the augmented language by definitions.

We moreover let

$$(\overline{a})^{\mathfrak{M}_G} = a^G \qquad \text{for each } a \in M \tag{1}$$

Thus every formula over $L_{\text{Set},M}$ says something about $M[G]$.[†]

**Caution.** It is important to note that even though the names $\overline{a}$ were "built" by importing into $L_{\text{Set}}$ names of objects of $M$, they are primarily used to name – *via the interpretation* (1) – objects of $M[G]$, *not* objects of $M$.

Whenever we interpret a formula in the structure $\mathfrak{M} = (M, U, \in)$, the names $\overline{a}, \ldots$ are interpreted as $(\overline{a})^{\mathfrak{M}} = a, \ldots$.[‡]

Of course, *in a roundabout way*, using the "caret" (cf. VIII.2.6), certain formal constants will be interpreted, *via* (1), into members of $M$:

$$(\overline{\hat{a}})^{\mathfrak{M}_G} = (\hat{a})^G = a \qquad \text{(cf. VIII.2.8)}$$

After all, $M \subseteq M[G]$.

*Under the interpretation* of $L_{\text{Set},M}$ in $\mathfrak{M}_G$ above, some names are interpreted as objects that are not in $M$. For example, we have seen circumstances under which an $M$-generic set $G$ is not a member of $M$ (VIII.1.9), yet there is a name for $G$ in $L_{\text{Set},M}$, namely, $\overline{\Gamma}$ (VIII.2.8).

We will find the following notation convenient:

**VIII.3.1 Definition.** For any $M$-generic $G$, $L_{\text{Set}}$ formula $\mathscr{A}(x_1, x_2, \ldots, x_n)$,[§] and $a_1, \ldots, a_n$ in $M$ we write

$$G \models \mathscr{A}(\overline{a_1}, \overline{a_2}, \ldots, \overline{a_n}) \tag{1}$$

or

$$G \models \mathscr{A}[\![\, a_1{}^G, a_2{}^G, \ldots, a_n{}^G \,]\!]$$

as a shorthand for

$$\models_{\mathfrak{M}_G} \mathscr{A}(\overline{a_1}, \overline{a_2}, \ldots, \overline{a_n}) \tag{2}$$

or

$$\models_{\mathfrak{M}_G} \mathscr{A}[\![\, a_1{}^G, a_2{}^G, \ldots, a_n{}^G \,]\!] \quad \text{(cf. I.5.17)}$$ □

[†] This procedure justifies the name "interpretation" for the function $x \mapsto x^G$.

[‡] E.g., in VIII.4.10.

[§] Under the term "$L_{\text{Set}}$ formula" we include formulas over $L_{\text{Set}}$ that may contain defined symbols. However these formulas must have *no* $M$-symbols $\overline{a}$, etc.

To a person living in $\mathbb{U}_A$, (2), and hence also (1), above mean the same thing as (cf. VI.8.4)

$$\models_{\mathbb{U}_A} \mathscr{A}^{M[G]} \llbracket a_1^G, a_2^G, \ldots, a_n^G \rrbracket$$

We will usually write the above using round brackets (*argot*). Similarly, one abuses notation slightly and writes

$$\models_{\mathfrak{M}_G} \mathscr{A}(a_1^G, a_2^G, \ldots, a_n^G) \tag{3}$$

instead of (2). However, to the right of $\models$ one normally expects to see a well-formed formula over our language, here $L_{\text{Set},M}$. Thus, a "real" object (from the structure $\mathfrak{M}_G$) can appear in a formula only by its formal name, $\overline{a}$, rather than by an informal name such as $a^G$, unless one writes in mixed mode using $\llbracket \ldots \rrbracket$ brackets.[†]

**VIII.3.2 Definition (Weak Forcing).** Let $M$ be a CTM and $\mathfrak{P} \in M$, while $p \in |\mathfrak{P}|$. For any $L_{\text{Set}}$ formula $\mathscr{A}(x_1, x_2, \ldots, x_n)$ and $a_i \in M$ we write

$$p \Vdash^w \mathscr{A}(\overline{a_1}, \overline{a_2}, \ldots, \overline{a_n}) \tag{1}$$

pronounced *p weakly forces the sentence* $\mathscr{A}(\overline{a_1}, \overline{a_2}, \ldots, \overline{a_n})$, to mean

$$(\forall G \subseteq |\mathfrak{P}|)\Big(G \text{ is } M\text{-generic } \wedge p \in G \text{ implies } G \models \mathscr{A}(\overline{a_1}, \overline{a_2}, \ldots, \overline{a_n})\Big)$$

Ideally one ought to use a subscript "$(M, \mathfrak{P})$" to the symbol "$\Vdash^w$", but such pedantry is almost never practised or needed. □

In conformity with the mixed-mode notation of VIII.3.1, we may also write instead of (1)

$$p \Vdash^w \mathscr{A}\llbracket a_1, a_2, \ldots, a_n \rrbracket \tag{2}$$

Note that since (1) is to be investigated within $M$, each $\overline{a_i}$ is interpreted as $a_i$ in $M$, which leads to (2). One then abuses notation and uses round brackets in (2) (more on this below).

Weak forcing is due to Feferman (1965). Intuitively, one can think of $p$ as "a finite amount of information" that is *sufficient* to make good the claim "$\mathscr{A}(\overline{a_1}, \overline{a_2}, \ldots, \overline{a_n})$ is true in $G$"[‡] in all the infinite (generic) extensions of $p$.[§] In effect, $p$ forces the truth of $\mathscr{A}(\overline{a_1}, \overline{a_2}, \ldots, \overline{a_n})$ in $M[G]$. Note that an inhabitant of $M$ can write down (1), but it is unclear *a priori* just how he might verify it or refute it, for he has no knowledge, in general (cf. VIII.1.9), of generic

[†] This same *apparent* hairsplitting is what made us import constants in I.5.4 towards defining the Tarski semantics for first order languages.

[‡] In the jargon of VIII.3.1.

[§] Looking back to VIII.1.9, this distinction between finite and infinite "amounts of information" is aptly motivated.

sets except by (formal) name – all he knows on faith is that generic sets are objects found beyond the universe he lives in. Yet we will see in the next section that this apparent dependence of forcing on $G$-sets and knowledge of "things outside $M$" can be circumvented.

We state here a few basic properties of $\Vdash^w$, all due to Cohen. Monotonicity (2) in VIII.3.3 below, and the definability and truth lemmata below, will be the ticket for the mathematician in $M$ to do forcing within his universe.

☡ In most cases below we write $c$ or $c^G$ (depending on target structure) instead of $\overline{c}$ in formulas. This notational simplification (*argot*) is achieved by using mixed-mode notation, but employing round brackets nevertheless. ☡

**VIII.3.3 Lemma (Cohen).** *Let $M$ be a CTM and $\mathfrak{P} \in M$, while $p \in |\mathfrak{P}|$ and $q \in |\mathfrak{P}|$. For any sentences $\mathscr{A}, \mathscr{B}$ over $L_{Set,M}$ the following hold:*

(1) Consistency: *We cannot have both $p \Vdash^w \mathscr{A}$ and $p \Vdash^w \neg\mathscr{A}$.*
(2) Monotonicity: *$p \Vdash^w \mathscr{A}$ and $q \leq p$ imply $q \Vdash^w \mathscr{A}$.*
(3) *$p \Vdash^w \mathscr{A} \wedge \mathscr{B}$ iff $p \Vdash^w \mathscr{A}$ and $p \Vdash^w \mathscr{B}$.*

*Proof.* (1): We cannot have both $\models_{\mathfrak{M}_G} \mathscr{A}$ and $\models_{\mathfrak{M}_G} \neg\mathscr{A}$.

(2): Any $M$-generic $G$ is a filter, and hence $q \in G$ implies $p \in G$.

(3): $\models_{\mathfrak{M}_G} \mathscr{A} \wedge \mathscr{B}$ iff $\models_{\mathfrak{M}_G} \mathscr{A}$ and $\models_{\mathfrak{M}_G} \mathscr{B}$. □

**VIII.3.4 Lemma (Definability Lemma).** *We fix a CTM $M$ and a notion of forcing $\mathfrak{P} \in M$. For any $\mathscr{A}(x_1, \ldots, x_n)$ over $L_{\mathrm{Set},M}$ there is a $\mathscr{B}(y, x_1, \ldots, x_n)$ over $L_{\mathrm{Set},M}$ such that for all $p \in |\mathfrak{P}|$ and $x_1, \ldots, x_n$ in $M$,*

$$\Big(p \Vdash^w \mathscr{A}(x_1, \ldots, x_n)\Big) \leftrightarrow \mathscr{B}^M(p, x_1, \ldots, x_n)$$

*holds in $\mathbb{U}_A$.*

☡ Granting the lemma, a being in $M$ can verify the right hand side of the above equivalence (hence also the left) *working in his world $M$* with the unrelativized $\mathscr{B}$ (cf. VI.8.4). ☡

The following lemma says that truth in $\mathfrak{M}_G$ can be certified by working with a finite approximation of $G$.

**VIII.3.5 Lemma (Truth Lemma).** *Let $M$ be a CTM, and $\mathfrak{P} \in M$ be a notion of forcing. For any $M$-generic $G \subseteq |\mathfrak{P}|$ and any formula $\mathscr{A}(\vec{x})$ over $L_{\mathrm{Set},M}$,*

$$\textit{for all } x_i \in M, \qquad \mathscr{A}^{M[G]}(x_1^G, \ldots, x_n^G) \leftrightarrow (\exists p \in G) p \Vdash^w \mathscr{A}(\vec{x}_n)$$

*holds in $\mathbb{U}_A$.*

The last two lemmata are proved in Section VIII.5 with the help of the "original" concept of Cohen's (strong) forcing.

## VIII.4. Strong Forcing

We define here Cohen's strong forcing relation, a syntactic concept that does not refer to generic sets and therefore can be defined within $\mathbb{U}_A$ or, indeed, within $M$.

We will use the symbol "$\Vdash$" for strong forcing, without qualifying superscripts or subscripts as to its "strength". In fact it will be shown that for any sentence over $L_{\mathrm{Set},M}$ and $p \in |\mathfrak{P}|$,

$$p \Vdash^w \mathscr{A} \quad \text{iff} \quad \Big(p \Vdash \neg\neg\mathscr{A}\Big)^M \tag{1}$$

The form of (1) immediately suggests that unlike $\Vdash^w$ – this being helped by its semantical definition – $\Vdash$ does *not* subscribe to the proposition that an even number of $\neg$ symbols at the front of a formula can be dropped.

We will attempt to motivate the definition of the version of $\Vdash$ we use here. This is the one in Shoenfield (1971) and is probably the user-friendliest in the literature (compare with the versions in Cohen (1963) and Kunen (1980)[†]). The reader is cautioned not to expect our motivational overture to unambiguously lead to a unique choice of definition of $\Vdash$. Even the auxiliary relation $x \in_p y$ introduced below can be defined in different ways (see, e.g., Shoenfield (1967 vs. 1971)).

The crucial concept in motivating the definition of $\Vdash$ is that by using it, in $M$, we can effect a syntactic approximation to truth in $M[G]$, i.e., an approximation to what

$$G \models \mathscr{A}(\overline{a_1}, \ldots, \overline{a_n})$$

or, more generally ($\mathscr{A}$ is over $L_{\mathrm{Set}}$),

$$G \models \mathscr{A}(x_1, \ldots, x_n)$$

means.

We begin by introducing a finite version of $x \in_G y$:

[†] Not only are the various versions of strong forcing not created equal in terms of definitional complexity, but this is also true in terms of their behaviour. For example, in the version in Kunen (1980), rather than (1) above one proves $p \Vdash^w \mathscr{A}$ iff $\big(p \Vdash \mathscr{A}\big)^M$.

**VIII.4.1 Definition.** Let $\mathfrak{P}$ be a PO set. With $p \in |\mathfrak{P}|$ and quantification over $|\mathfrak{P}|$ we introduce the abbreviation

$$x \in_p y \quad \text{stands for} \quad (\exists q \geq p)\langle x, q\rangle \in y \qquad \square$$

Suppose that $\mathfrak{P} \in M$, where $M$ is a CTM of ZF. Thus, $x \in_p y$ is similar to $x \in_G y$. In each case, the membership in $y$ (via $\in_G$ or $\in_p$) is settled by looking at *one* appropriate *finite* piece of information that is part of $G$ or $p$ (recall that when $q \geq p$, $q$ contains less information than $p$ – cf. VIII.1.3). In the case of $\in_p$, however, we even *start* with a finite amount of information, $p$, rather than $G$.

This relation is not explicitly defined in Shoenfield (1971), but is used there in a crucial way to define $p \Vdash x \in y$ (see below). By contrast, in Shoenfield (1967) $x \in_p y$ is explicitly introduced, but there it abbreviates something else, namely, $(\forall q \leq p)\langle x, q\rangle \in y$; i.e., one looks at all *finite extensions* of $p$ in order to settle whether $x \in_p y$.

The above considerations complement our earlier comment that this motivational discussion will not deliver the definition of $\Vdash$ uniquely. In the end, the definition of $\Vdash$ is meant to make the following three lemmata and (1) above true. Any definition that works will do.

In the four lemmata immediately below, $M$ is an arbitrary set, possibly empty, whose sole purpose is to enrich $L_{\text{Set}}$ with a number of additional constants. It bears no relation to $\mathfrak{P}$ in general.

**VIII.4.2 Lemma (Definability Lemma – Strong Forcing Version).** *Let $M$ be a set, and $\mathfrak{P}$ a PO set.*

*For any $\mathscr{A}(x_1, \ldots, x_n)$ over $L_{\text{Set},M}$ there is an $\mathscr{A}'(y, x_1, \ldots, x_n)$ over $L_{\text{Set},M}$ such that for all $p \in |\mathfrak{P}|$ the following holds in $\mathbb{U}_A$:*

$$\Big(p \Vdash \mathscr{A}(x_1, \ldots, x_n)\Big) \leftrightarrow \mathscr{A}'(p, x_1, \ldots, x_n)$$

Just like $\vdash$ and $\models$, $\Vdash$ and $\Vdash^w$ apply to everything to their right (they have lowest priority, hence maximum scope). This explains the brackets around $p \Vdash \mathscr{A}(x_1, \ldots, x_n)$ above.

**VIII.4.3 Lemma (Monotonicity Lemma – Strong Forcing Version).** *Let $M$ be a set, and $\mathfrak{P}$ a PO set. Assume that $p \in |\mathfrak{P}|$ and $q \in |\mathfrak{P}|$ with $q \leq p$. Then for any formula $\mathscr{A}(\vec{x}_n)$ over $L_{\text{Set},M}$, the following holds in $\mathbb{U}_A$:*

$$\Big(p \Vdash \mathscr{A}(\vec{x}_n)\Big) \to \Big(q \Vdash \mathscr{A}(\vec{x}_n)\Big)$$

**VIII.4.4 Lemma (Consistency Lemma).** *Let $M$ be a set, $\mathfrak{P}$ a PO set, and $p \in |\mathfrak{P}|$. Then for any formula $\mathscr{A}(x_1, \ldots, x_n)$ over $L_{\mathrm{Set},M}$ and any $x_1, \ldots, x_n$ it is true in $\mathbb{U}_A$ that we cannot have both $p \Vdash \mathscr{A}(x_1, \ldots, x_n)$ and $p \Vdash \neg\mathscr{A}(x_1, \ldots, x_n)$.*

**VIII.4.5 Lemma (Quasi-completeness Lemma).** *Let $M$ be a set, and $\mathfrak{P}$ a PO* set. *For any $p \in |\mathfrak{P}|$ and formula $\mathscr{A}(\vec{x}_n)$ over $L_{\mathrm{Set},M}$, the following holds in $\mathbb{U}_A$: There is a $q \leq p$, depending on $\vec{x}_n$, such that*

$$\Big(q \Vdash \mathscr{A}(\vec{x}_n)\Big) \vee \Big(q \Vdash \neg\mathscr{A}(\vec{x}_n)\Big)$$

**VIII.4.6 Remark.** In other words, for any fixed $\vec{x}_n$, the set

$$\Big\{p \in |\mathfrak{P}| : \Big(p \Vdash \mathscr{A}(\vec{x}_n)\Big) \vee \Big(p \Vdash \neg\mathscr{A}(\vec{x}_n)\Big)\Big\}$$

is dense. If $M$ is a CTM of ZF − P, $\vec{x}_n$ is in $M$, and $\mathfrak{P} \in M$, then relativizing to $M$ yields

$$\Big(\Big\{p \in |\mathfrak{P}| : \Big(p \Vdash \mathscr{A}(\vec{x}_n)\Big) \vee \Big(p \Vdash \neg\mathscr{A}(\vec{x}_n)\Big)\Big\} \text{ is dense}\Big)^M$$

Hence, since being dense is absolute for such a CTM (Exercise VIII.3),

$$\Big\{p \in |\mathfrak{P}| : \Big(p \Vdash \mathscr{A}(\vec{x}_n)\Big)^M \vee \Big(p \Vdash \neg\mathscr{A}(\vec{x}_n)\Big)^M\Big\} \text{ is a dense set in } M. \quad \square$$

**VIII.4.7 Lemma (Truth Lemma – Strong Forcing Version).** *Let $M$ be a CTM, and $\mathfrak{P} \in M$ be a notion of forcing. For any $M$-generic $G \subseteq |\mathfrak{P}|$ and any formula $\mathscr{A}(\vec{x}_n)$ over $L_{Set,M}$, it is true in $\mathbb{U}_A$ (provable with no more than the* ZF *axioms) that*

$$(\forall \vec{x}_n \in M^n)\Big(\mathscr{A}^{M[G]}(x_1^G, \ldots, x_n^G) \leftrightarrow (\exists p \in G)\big(p \Vdash \mathscr{A}(\vec{x}_n)\big)^M\Big)$$

The definition of $\Vdash$ will be given syntactically in the metatheory – specifically, within $\mathbb{U}_A$ (using no more than the ZF axioms) – in VIII.4.8 below. We continue our work, pretending that we live in $M$, towards motivating the final definition.

Defining $p \Vdash U(\overline{a})$ is easy: we will let $p \Vdash U(\overline{a})$ be true iff $U(\overline{a})$ is true in $M$ (which is so, by VIII.2.9, iff $U(\overline{a})$ is true in $M[G]$).

*Syntactically*, we will let the expression $p \Vdash U(x)$ – where $x$ is a variable – just stand for $U(x)$.

Next we search for a good definition for $p \Vdash \overline{a} \in \overline{b}$ and $p \Vdash \overline{a} = \overline{b}$,[†] or, more generally (with free variables), of $p \Vdash x \in y$ and $p \Vdash x = y$.

So, what does $\models_{\mathfrak{M}_G} \overline{a} \in \overline{b}$ mean? It means that $a^G \in b^G$ is true, that is, $a \in_G b$ is true. This is, trivially, equivalent to (cf. I.6.2)

$$(\exists z)(z = a \wedge z \in_G b) \tag{1}$$

To obtain a finite approximation of (1) we replace $z = a$ and $z \in_G b$ by finite approximations (we use strong forcing to approximate $z = a$). This leads to $(\exists z)(z \in_p b \wedge p \Vdash z = a)$, or, in the free variables version,

$$p \Vdash x \in y \quad \text{means} \quad (\exists z)(z \in_p y \wedge p \Vdash z = x) \tag{2}$$

More explicitly (by VIII.4.1),

$$p \Vdash x \in y \quad \text{means} \quad (\exists z)(\exists q \geq p)(\langle z, q\rangle \in y \wedge p \Vdash z = x) \tag{3}$$

We have already indicated that we will define what $p \Vdash x \neq y$ means and then obtain the meaning for $p \Vdash x = y$ indirectly. Thus, before we focus on $\neq$, let us reflect on how to get $p \Vdash \neg\mathscr{A}$ from $p \Vdash \mathscr{A}$ in general. Unlike the case for $\models$, we must *not* set[‡]

$$p \Vdash \neg\mathscr{A} \quad \text{iff} \quad \neg p \Vdash \mathscr{A}$$

for it is conceivable that the $p$ does not force the truth of $\mathscr{A}$, simply because it does not contain enough information to do so. Thus we need to know that no amount of *additional* finite information (any $q$ such that $q \leq p$) will help to force $\mathscr{A}$. Then we can proclaim that $p$ forces $\neg\mathscr{A}$. Thus, we will adopt

$$p \Vdash \neg\mathscr{A} \quad \text{iff} \quad (\forall q \leq p)\neg q \Vdash \mathscr{A} \tag{4}$$

With this settled, what does $\models_{M[G]} \overline{a} \neq \overline{b}$ mean? It means that $a^G = b^G$ is false, and therefore one of the following cases obtains:

(i) $U(a) \wedge U(b) \wedge a \neq b$ (recall that $U(a)$ iff $U(a^G)$)
(ii) $U(a) \wedge \neg U(b)$
(iii) $\neg U(a) \wedge U(b)$
(iv) $(\exists z)\Big((z \in a^G \wedge z \notin b^G) \vee (z \in b^G \wedge z \notin a^G)\Big)$

[†] Actually, it turns out to be technically somewhat more convenient to look for a definition of $p \Vdash \overline{a} \neq \overline{b}$, viewing $\neq$ as the primary (in)equality predicate and $=$ as a derived one.

[‡] The first $\neg$ is formal, part of the formula $\neg\mathscr{A}$. The second is metamathematical. Some writers use $p \not\Vdash \mathscr{A}$ instead.

Condition (iv) is equivalent to

$$(\exists z)\Big((z \in_G a \wedge z \notin_G b) \vee (z \in_G b \wedge z \notin_G a)\Big) \tag{5}$$

where we have written $x \notin_G y$ for $\neg x \in_G y$. A finite approximation of (5) that (as we will see) works is obtained by using $\in_p$ for the positive cases and $p \Vdash$ for the negative cases. We are ready to summarize in a definition.

**VIII.4.8 Definition. (Shoenfield (1971).)** We fix a PO set $\mathfrak{P} = \langle P, <, 1\rangle$ and a set $M$ – possibly empty, a provider of constants – and define within $\mathbb{U}_A$ (using no more than the ZF − P axioms) the symbol $p \Vdash \mathscr{A}$, for any formula of $L_{\mathrm{Set},M}$. We do so by induction on formulas:

(a) $p \Vdash U(x)$ stands for $U(x)$.
(b) $p \Vdash x \in y$ is given by (2) (p. 535) (equivalently, (3), p. 535).
(c) $p \Vdash x \neq y$ stands for

$$\begin{gathered}(U(x) \wedge U(y) \wedge x \neq y) \vee (U(x) \wedge \neg U(y)) \vee (\neg U(x) \wedge U(y)) \\ \vee\ (\exists z)\Big((z \in_p x \wedge p \Vdash z \notin y) \vee (z \in_p y \wedge p \Vdash z \notin x)\Big)\end{gathered}$$

(d) $p \Vdash \neg\mathscr{A}$ iff $(\forall q \leq p)\neg q \Vdash \mathscr{A}$.
(e) $p \Vdash \mathscr{A} \vee \mathscr{B}$ iff $p \Vdash \mathscr{A}$ or $p \Vdash \mathscr{B}$.
(f) $p \Vdash (\exists x)\mathscr{A}[x]$ iff $(\exists x)\big(p \Vdash \mathscr{A}[x]\big)$. □

**VIII.4.9 Remark.** In (b) and (c) above an occurrence of $q \Vdash u \notin w$ is (in view of (d)) an abbreviation for

$$(\forall r \leq q)\neg r \Vdash u \in w \tag{6}$$

while (since $u = w$ is an abbreviation of $\neg u \neq w$) $q \Vdash u = w$ is an abbreviation for

$$(\forall r \leq q)\neg r \Vdash u \neq w \tag{7}$$

Using (6) and (7), we can thus rewrite clauses (b) and (c) of the definition to read

$$p \Vdash x \in y \quad \text{abbreviates} \quad (\exists z)(\exists q \geq p)(\langle z, q\rangle \in y \wedge (\forall r \leq p)\neg r \Vdash z \neq x) \tag{8}$$

and

$$
\begin{aligned}
p \Vdash x \neq y \quad & \text{abbreviates} \\
& (U(x) \wedge U(y) \wedge x \neq y) \vee (U(x) \wedge \neg U(y)) \vee (\neg U(x) \wedge U(y)) \vee \\
& \quad (\exists z)(\exists q \geq p)\Big((\langle z, q\rangle \in x \wedge (\forall r \leq p)\neg r \Vdash z \in y) \vee \\
& \qquad\qquad (\langle z, q\rangle \in y \wedge (\forall r \leq p)\neg r \Vdash z \in x)\Big)
\end{aligned} \tag{9}
$$

respectively. This now makes sense out of Definition VIII.4.8(b)–(c), since (8) and (9) constitute a simultaneous recursion in the sense of VI.2.40.

More rigorously, then, what Definition VIII.4.8(b) and (c) really mean is that we employ the *abbreviations*

$$
\text{for any } p \in |\mathfrak{P}|, \qquad p \Vdash x \in y \text{ stands for } \mathbb{I}n(p, x, y) = 0 \tag{10}
$$

and

$$
\text{for any } p \in |\mathfrak{P}|, \qquad p \Vdash x \neq y \text{ stands for } \mathbb{N}e(p, x, y) = 0 \tag{11}
$$

where the functions $\lambda pxy.\mathbb{I}n(p, x, y)$ and $\lambda pxy.\mathbb{N}e(p, x, y)$ (with right field $\{0, 1\}$) are defined in $\mathbb{U}_A$ by the simultaneous recursion $(8') + (9')$ below, mimicking (8) and (9):

$$
\mathbb{I}n(p, x, y) = \begin{cases} 0 & \text{if } p \in |\mathfrak{P}| \wedge \\ & \quad (\exists z)(\exists q \geq p)(\langle z, q\rangle \in y \wedge (\forall r \leq p)\mathbb{N}e(r, z, x) = 1) \\ 1 & \text{otherwise (this includes the case } p \notin |\mathfrak{P}|) \end{cases} \tag{8$'$}
$$

and

$$
\mathbb{N}e(p, x, y) = \begin{cases} 0 & \text{if } p \in |\mathfrak{P}| \wedge \Big((U(x) \wedge U(y) \wedge x \neq y) \vee (U(x) \wedge \neg U(y)) \\ & \vee (\neg U(x) \wedge U(y)) \\ & \quad \vee (\exists z)(\exists q \geq p)\big[\big(\langle z, q\rangle \in x \wedge (\forall r \leq p)\mathbb{I}n(r, z, y) = 1\big) \\ & \vee \big(\langle z, q\rangle \in y \wedge (\forall r \leq p)\mathbb{I}n(r, z, x) = 1\big)\big]\Big) \\ 1 & \text{otherwise} \end{cases} \tag{9$'$}
$$

That the recursion $(8')$–$(9')$ is legitimate follows from the following considerations: We note that $(8')$ implies $z \in \operatorname{dom}(y)$ (by $\langle z, q\rangle \in y$) and hence $\max(\rho(z), \rho(x)) < \max(\rho(x), \rho(y))$. Similarly, $(9')$ implies $z \in \operatorname{dom}(x)$ (by $\langle z, q\rangle \in x$) or $z \in \operatorname{dom}(y)$ (by $\langle z, q\rangle \in y$); thus $\max(\rho(z), \rho(y)) < \max(\rho(x), \rho(y))$ and $\max(\rho(z), \rho(x)) < \max(\rho(x), \rho(y))$ respectively. It follows that the recursion is with respect to the relation

$$\langle p, u, v\rangle \mathbb{P} \langle q, x, y\rangle \quad \text{iff} \quad \{p, q\} \subseteq |\mathfrak{P}| \wedge \max(\rho(u), \rho(v)) < \max(\rho(x), \rho(y))$$

which has MC and is left-narrow (verify!) as required.

We now recast the entire Definition VIII.4.8 in a rigorous light: (a) and (d)–(f) remain the same, giving meaning to the left hand side in terms of the right hand side. (b) and (c) are now (10) and (11) above.

By the absoluteness results of Section VI.8 (in particular, absoluteness of ranks; cf. also VI.8.23 and VI.8.24), both $\mathbb{I}n$ and $\mathbb{N}e$ are absolute for any CTM $M$ of ZF − P. Let then $M$ be such a CTM with $\mathfrak{P} \in M$. Relativizing to $M$, we have, for all $a$ and $b$ in $M$ and $p \in |\mathfrak{P}|$,

$$\mathbb{I}n^M(p, a, b) = \mathbb{I}n(p, a, b) \quad \text{and} \quad \mathbb{N}e^M(p, a, b) = \mathbb{N}e(p, a, b) \tag{12}$$

or

$$\mathbb{I}n^M = \mathbb{I}n \restriction M \quad \text{and} \quad \mathbb{N}e^M = \mathbb{N}e \restriction M \tag{13}$$

□

*Proof of Lemma VIII.4.2.* We do induction on formulas. A trivial preliminary remark is that "stands for" can be replaced by "↔". For example, (10) can be rewritten as

$$\text{For any } p \in |\mathfrak{P}|, \qquad \Big(p \Vdash x \in y\Big) \leftrightarrow \mathbb{I}n(p, x, y) = 0$$

for if we replace the abbreviation $p \Vdash x \in y$ by what it abbreviates, we get a tautology.

For the basis, $\mathscr{A}$ may be

(i) $U(x)$. We then take $\mathscr{A}'(p, x) \equiv U(x)$.
(ii) $x \in y$. Then use $\mathscr{A}'(p, x, y) \equiv \mathbb{I}n(p, x, y) = 0$.
(iii) $x \neq y$. Then use $\mathscr{A}'(p, x, y) \equiv \mathbb{N}e(p, x, y) = 0$.

For the induction steps, $\mathscr{A}$ may be

(I) $\neg\mathscr{B}(\vec{x})$. Then we can let $\mathscr{A}'(p, \vec{x}) \equiv (\forall q \leq p)\mathscr{B}'(q, \vec{x})$.
(II) $\mathscr{B} \vee \mathscr{C}$. Then we let $\mathscr{A}' \equiv \mathscr{B}' \vee \mathscr{C}'$.
(III) $(\exists y)\mathscr{B}(y, \vec{x})$. Then we set $\mathscr{A}'(p, \vec{x}) \equiv (\exists y)\mathscr{B}'(p, y, \vec{x})$. □

**VIII.4.10 Corollary.** *Let $M$ be a CTM of ZF − P, and $\mathfrak{P} \in M$ a notion of forcing. For any formula $\mathscr{A}(\vec{x}_n)$ over $L_{Set}$ there is a formula $\mathscr{B}(y, \vec{x}_n)$ over*

$L_{\text{Set}}$ *such that for all* $a_1, \ldots, a_n$ *in* $M$ *and all* $p \in |\mathfrak{P}|$,

$$\models_{\mathbb{U}_A} \Big(p \Vdash \mathscr{A}(\overline{a_1}, \ldots, \overline{a_n})\Big)^M \quad \textit{iff} \quad \models_{\mathfrak{M}} \mathscr{B}\llbracket\, p, \vec{a}_n \,\rrbracket$$

*where* $\mathfrak{M} = (M, U, \in)$.

*Proof.* Relativizing VIII.4.2 to $M$, we get

$$(\forall p \in |\mathfrak{P}|)(\forall \vec{x}_n \in M)\Big(\Big(p \Vdash \mathscr{A}(x_1, \ldots, x_n)\Big)^M \leftrightarrow \mathscr{A}'(p, x_1, \ldots, x_n)^M\Big)$$

in particular, for any $p \in |\mathfrak{P}|$ and constants $\overline{a_1}, \ldots, \overline{a_n}$ in $M$,[†]

$$\Big(p \Vdash \mathscr{A}(\overline{a_1}, \ldots, \overline{a_n})\Big)^M \leftrightarrow \mathscr{A}'(p, \overline{a_1}, \ldots, \overline{a_n})^M$$

Setting $\mathscr{B} \equiv \mathscr{A}'$ and rewriting the right hand side of the above in $\llbracket \ldots \rrbracket$ notation, we are done. □

**Caution.** $p \Vdash U(x)$, $p \Vdash x \in y$, and $p \Vdash x \neq y$ are absolute for CTMs, as noted in VIII.4.9. Thus, e.g., $(p \Vdash x \in y)^M$ is equivalent to $p \Vdash x \in y$ for all $p, x, y$ in $M$. However, $p \Vdash \ldots$, in general, is *not* absolute.

*Proof of Lemma VIII.4.3.* We do induction on formulas, following Definition VIII.4.8. Now, $\mathscr{A}$ may be one of

(i) $U(x)$: Then the result is immediate.
(ii) $x \in y$: Let $p \Vdash x \in y$ and $s \leq p$. By assumption we have (8) of Remark VIII.4.9. This remains valid if we replace the letter $p$ by $s$ throughout (transitivity of $\leq$).
(iii) $x \neq y$: Exactly as in the previous case (using (9) of VIII.4.9)

For the induction steps, $\mathscr{A}$ may be

(I) $\neg\mathscr{B}$: Let $q \leq p$ and $(\forall r \leq p)\neg r \Vdash \mathscr{B}$. Then $(\forall r \leq q)\neg r \Vdash \mathscr{B}$, that is, $q \Vdash \neg\mathscr{B}$. (The I.H. was not used)
(II) $\mathscr{B} \vee \mathscr{C}$: Exercise.
(III) $(\exists y)\mathscr{B}(y, \vec{x})$: Let $q \leq p$ and $p \Vdash \mathscr{A}$. That is, $(\exists y)p \Vdash \mathscr{B}(y, \vec{x})$. By the I.H., $(\exists y)q \Vdash \mathscr{B}(y, \vec{x})$. □

*Proof of Lemma VIII.4.4.* Fix $\vec{x}$. Then $p \Vdash \neg\mathscr{A}(\vec{x})$ means $(\forall q \leq p)q \nVdash \mathscr{A}(\vec{x})$. In particular, $p \nVdash \mathscr{A}(\vec{x})$. □

[†] We have opted here for the notation "$\mathscr{A}'(\ldots)^M$" rather than the awkward "$(\mathscr{A}')^M(\ldots)$".

*Proof of Lemma VIII.4.5.* Fix $\vec{x}$ and $p \in |\mathfrak{P}|$. If $p \Vdash \neg\mathscr{A}(\vec{x})$, then we are done with $q = p$. Else, there is a $q \le p$ such that $q \Vdash \mathscr{A}(\vec{x})$ by VIII.4.8 – the $\neg$ -case. □

*Proof of Lemma VIII.4.7.* Fix an $M$-generic set $G$. We do induction on formulas, following Definition VIII.4.8. For the *basis* we do induction on $\max(\rho(x), \rho(y))$. Now, $\mathscr{A}$ may be one of

(i) $U(x)$: Trivial. Forcing = truth in this case.

(ii) $x \in y$:

$\rightarrow$: We fix $x$ and $y$ in $M$ such that $x^G \in y^G$ is true. Thus, $(\exists z)(z = x \wedge z \in_G y)$ (cf. (1) of p. 535). Let $c$ (auxiliary constant) be a $z$ that works. By the I.H. (on $\max(\rho(x), \rho(y))$), let $p \in G$ be such that[†]

$$p \Vdash c = x \tag{$a$}$$

Let also $q \in G$ such that $\langle c, q\rangle \in y$. There is an $r \in G$ that witnesses compatibility of $p$ and $q$. Then $r \Vdash c = x$ by VIII.4.3 and ($a$) above. Thus

$$(\exists z)(\exists q \ge r)(\langle z, q\rangle \in y \wedge r \Vdash z = x) \tag{$b$}$$

– in short, $(\exists r \in G) r \Vdash x \in y$.[‡]

$\leftarrow$: Let $x$ and $y$ be in $M$ and assume ($b$), with $r \in G$. Let $c$ work for $z$. Then $q \in G$ by filter properties; thus $c \in_G y$; hence

$$c^G \in y^G \tag{$d$}$$

Moreover, the I.H. (on $\max(\rho(x), \rho(y))$) implies that $c^G = x^G$. Combining with ($d$) (via the Leibniz axiom), we get $x^G \in y^G$.

(iii) $x \neq y$:

$\rightarrow$: We fix $x$ and $y$ in $M$ such that $x^G \neq y^G$ is true. We have cases:

(a) $U(x^G) \wedge U(y^G)$. Then $x = x^G$ and $y = y^G$ (VIII.2.9), and thus $x \neq y$. By VIII.4.8, any $p \in |\mathfrak{P}|$ satisfies $p \Vdash x \neq y$. Taking, for example, $p = 1$, we have such a $p$ in $G$.

(b) $U(x^G) \wedge \neg U(y^G)$. Then (VIII.2.9) $U(x) \wedge \neg U(y)$, and any $p \in |\mathfrak{P}|$ satisfies $p \Vdash x \neq y$ (VIII.4.8). We conclude as in the previous case.

(c) $\neg U(x^G) \wedge U(y^G)$. As above.

[†] The I.H. applies to atomic formulas, here $c \neq x$. However, it is all right to apply it to negated atomic formulas, here $c = x$, by the "$\neg$" case below.

[‡] By the remark following the proof of VIII.4.10, it is unnecessary to write $(r \Vdash x \in y)^M$.

(d) $\neg U(x^G) \wedge \neg U(y^G)$. Thus,

$$\begin{aligned}&\big(\exists z \in \mathrm{dom}(x) \cup \mathrm{dom}(y)\big)\\ &\quad\Big((z^G \in x^G \wedge z^G \notin y^G)\\ &\qquad \vee (z^G \in y^G \wedge z^G \notin x^G)\Big)\end{aligned} \tag{1}$$

For the sake of argument, say it is the first of the two ($\vee$-)cases of (1) above that holds for some $z$. Then $z \in_G x$, i.e., for some $p \in G$,

$$\langle z, p\rangle \in x \tag{2}$$

Moreover, since $\rho(z) < \rho(x)$ by (2), $\max(\rho(z), \rho(y)) < \max(\rho(x), \rho(y))$; thus the I.H. implies, for some $q \in G$,

$$q \Vdash z \notin y \tag{3}$$

Let $r \in G$ satisfy $r \leq q$ and $r \leq p$. Then (2) yields $z \in_r x$, and (3) yields $r \Vdash z \notin y$ by VIII.4.3. Thus $r \Vdash x \neq y$. The other case in (1) is entirely analogous.

$\leftarrow$: We fix $p \in G$ and $x$ and $y$ in $M$ such that $p \Vdash x \neq y$. We have cases.

(a′) $U(x) \wedge U(y)$. By VIII.4.8, $x \neq y$ holds. Since $x = x^G$ and $y = y^G$ (VIII.2.9), $x^G \neq y^G$ holds.

(b′) $U(x) \wedge \neg U(y)$. Then (VIII.2.9) $U(x^G) \wedge \neg U(y^G)$. Thus $x^G \neq y^G$ holds.

(c′) $\neg U(x) \wedge U(y)$. As above.

(d′) $\neg U(x) \wedge \neg U(y)$. By VIII.4.8,

$$\begin{aligned}&\big(\exists z \in \mathrm{dom}(x) \cup \mathrm{dom}(y)\big)\\ &\quad\Big((\exists q \geq p)(\langle z, q\rangle \in x \wedge p \Vdash z \notin y)\\ &\qquad \vee (\exists q \geq p)(\langle z, q\rangle \in y \wedge p \Vdash z \notin x)\Big)\end{aligned} \tag{4}$$

For the sake of argument, say it is the first of the two ($\vee$-)cases of (4) above that holds for some $z$. Then $z \in_G x$, since $q \in G$ by filter properties; hence

$$z^G \in x^G \tag{5}$$

$\rho(z) < \rho(x)$ by $z \in \mathrm{dom}(x)$ implies $\max(\rho(z), \rho(y)) < \max(\rho(x), \rho(y))$; hence, from $p \Vdash z \notin y$ and the I.H.,

$$z^G \notin y^G \tag{6}$$

(5) and (6) now yield $x^G \neq y^G$. The other case in (4) is entirely analogous.

For the induction steps, with respect to formulas, $\mathscr{A}$ may be

(I) $\neg\mathscr{B}(\vec{x}_n)$: Fix $x_i$, $i = 1, \ldots, n$ in $M$. By Remark VIII.4.6 and $M$-genericity of $G$,

$$(\exists p \in G)\Big(\big(p \Vdash \mathscr{B}(\vec{x}_n)\big)^M \vee \big(p \Vdash \neg\mathscr{B}(\vec{x}_n)\big)^M\Big) \tag{7}$$

$\rightarrow$: Assume $\neg\mathscr{B}^{M[G]}(x_1^G, \ldots, x_n^G)$. Let $q \in G$ make (7) true. Then $\big(q \Vdash \neg\mathscr{B}(\vec{x}_n)\big)^M$, since the alternative and the I.H. would yield $\mathscr{B}^{M[G]}(x_1^G, \ldots, x_n^G)$, contradicting the assumption.

$\leftarrow$: Let $p \in G$ be such that $\big(p \Vdash \neg\mathscr{B}(\vec{x}_n)\big)^M$. Then (VIII.4.4) $\big(p \nVdash \mathscr{B}(\vec{x}_n)\big)^M$.

Is it possible that, for some $r \in G$, $\big(r \Vdash \mathscr{B}(\vec{x}_n)\big)^M$? Well, if so, let $s \in G$ witness the compatibility of $p$ and $r$. Then (VIII.4.3)

$$\big(s \Vdash \mathscr{B}(\vec{x}_n)\big)^M \wedge \big(s \Vdash \neg\mathscr{B}(\vec{x}_n)\big)^M$$

contradicting VIII.4.4. Thus,

$$(\forall p \in G)\big(p \nVdash \mathscr{B}(\vec{x}_n)\big)^M$$

or

$$\neg(\exists p \in G)\big(p \Vdash \mathscr{B}(\vec{x}_n)\big)^M$$

By the I.H., this translates to "$\mathscr{B}^{M[G]}(x_1^G, \ldots, x_n^G)$ is false in $\mathbb{U}_A$". Hence $\neg\mathscr{B}(x_1^G, \ldots, x_n^G)^{M[G]}$ is true.

(II) $\mathscr{B} \vee \mathscr{C}$: Exercise.

(III) $(\exists y)\mathscr{B}(y, \vec{x})$: Fix $\vec{x}$ in $M$.

$\rightarrow$: Let

$$(\exists y \in M[G])\mathscr{B}^{M[G]}(y, x_1^G, \ldots, x_n^G) \tag{8}$$

be true. Let $y = a$ work above. Then for some $b$ in $M$, $a = b^G$ and

$$\mathscr{B}^{M[G]}(b^G, x_1^G, \ldots, x_n^G) \tag{9}$$

is true. By the I.H.,

$$(\exists p \in G)\big(p \Vdash \mathscr{B}(b, x_1, \ldots, x_n)\big)^M \tag{10}$$

is true; hence

$$(\exists p \in G)\big(p \Vdash (\exists y)\mathscr{B}(y, x_1, \ldots, x_n)\big)^M \tag{11}$$

is true, by VIII.4.8 ($\exists$-case).

$\rightarrow$: Let (11) hold for the given $\vec{x}$. Then (10) holds by VIII.4.8 ($\exists$-case) for some $b \in M$. Therefore, by the I.H., (9) holds. Thus we have (8). □

## VIII.5. Strong vs. Weak Forcing

We can now connect $\Vdash$ and $\Vdash^w$.

**VIII.5.1 Theorem.** *Fix a CTM M and a PO set $\mathfrak{P} \in M$. Then for any formula $\mathscr{A}(\vec{x}_n)$ over $L_{\mathrm{Set},M}$, and all $\vec{x}_n$ in M,* (1) *on p. 532 holds in $\mathbb{U}_A$.*

*Proof.* Fix $x_1, \ldots, x_n$ in $M$. We prove that

$$\Big(p \Vdash^w \mathscr{A}(\vec{x}_n)\Big) \leftrightarrow \Big(p \Vdash \neg\neg\mathscr{A}(\vec{x}_n)\Big)^M \tag{2}$$

holds in $\mathbb{U}_A$.

$\leftarrow$: Assume the right hand side of $\leftrightarrow$, and let $G \subseteq |\mathfrak{P}|$ be $M$-generic and $p \in G$ (cf. VIII.1.8). By VIII.4.7, $\neg\neg\mathscr{A}^{M[G]}(x_1^G, \ldots, x_n^G)$ is true; hence so is $\mathscr{A}^{M[G]}(x_1^G, \ldots, x_n^G)$. By Definition VIII.3.2, $p \Vdash^w \mathscr{A}(\vec{x}_n)$, since $G$ (with $p \in G$) was an arbitrary generic set.

$\rightarrow$: We prove the contrapositive, so let

$$\neg\Big(p \Vdash \neg\neg\mathscr{A}(\vec{x}_n)\Big)^M \tag{3}$$

Thus, for some $q \leq p$,

$$\Big(q \Vdash \neg\mathscr{A}(\vec{x}_n)\Big)^M \tag{4}$$

By VIII.1.8, let $G$ be $M$-generic and $q \in G$. By VIII.4.7, (4) yields the truth of

$$\neg\mathscr{A}^{M[G]}(x_1^G, \ldots, x_n^G)$$

By filter properties, $p \in G$. Definition VIII.3.2 then yields $\neg\big(p \Vdash^w \mathscr{A}(\vec{x}_n)\big)$. □

One now obtains the Lemmata VIII.3.4 and VIII.3.5 at once:

*Proof of Lemma VIII.3.4.* By VIII.5.1 and VIII.4.2 we can take

$$\mathscr{B}(p, \vec{x}) \equiv \big(p \Vdash \neg\neg\mathscr{A}(\vec{x})\big)$$ □

*Proof of Lemma VIII.3.5.* $\leftarrow$: Pick any $M$-generic $G$. Let $p \in G$, $x_i$ ($i = 1, \ldots, n$) be in $M$, and $p \Vdash^w \mathscr{A}(\vec{x}_n)$. By Definition VIII.3.2, $\mathscr{A}^{M[G]}(x_1^G, \ldots, x_n^G)$ holds.

$\rightarrow$: Pick any $M$-generic $G$ and $x_i$ $(i = 1, \ldots, n)$ in $M$. Assume now that $\mathscr{A}^{M[G]}(x_1^G, \ldots, x_n^G)$ holds. Then also $\big(\neg\neg\mathscr{A}(x_1^G, \ldots, x_n^G)\big)^{M[G]}$ holds. By VIII.4.7,

$$(\exists p \in G)\Big(p \Vdash \neg\neg\mathscr{A}(x_1, \ldots, x_n)\Big)^M$$

We are done by VIII.5.1. □

## VIII.6. $M[G]$ Is a CTM of ZFC If $M$ Is

Let $M$ be a CTM for ZFC, $\mathfrak{P} \in M$ be a notion of forcing in $M$, and $G \subseteq |\mathfrak{P}|$ be $M$-generic. We will show that $M[G]$ is also a CTM of ZFC, indeed the $\subseteq$-smallest.

So far we know that $M[G]$ is countable and transitive (VIII.2.11) and is a subset of any CTM $N$ such that $M \subseteq N$ and $G \in N$ (VIII.2.5). It remains to see that indeed it is a model of ZFC.

**VIII.6.1 Lemma.** *For any $x \in M$, $\rho(x^G) \leq \rho(x)$.*

*Proof.* We do $\in$-induction. If $U(x^G)$, then also $U(x)$; thus $\rho(x^G) = \rho(x) = 0$ VI.6.24). Next, assume that $\neg U(x^G)$. Then

$$\begin{aligned}\rho(x^G) &= \left(\bigcup_{y^G \in x^G} \rho(y^G)\right) + 1 \\ &\leq \left(\bigcup_{(\exists p \in G)\langle y, p\rangle \in x} \rho(y)\right) + 1 \qquad \text{by I.H.} \\ &\leq \left(\bigcup_{z \in x} \rho(z)\right) + 1 \qquad \text{since } \rho(y) < \rho(\langle y, p\rangle) \\ &= \rho(x)\end{aligned}$$

□

**VIII.6.2 Lemma.** $\mathrm{On}^M = \mathrm{On}^{M[G]}$.

*Proof.* $\mathrm{On}^M = \{x \in M : (x \in \mathrm{On})^M\} = \{x \in M : x \in \mathrm{On}\} = M \cap \mathrm{On}$, the second "=" by absoluteness of $(x \in \mathrm{On})$ for transitive classes. That is, $\mathrm{On}^M$ is the set of all *real*[†] ordinals found inside $M$. To an inhabitant of $M$, $\mathrm{On}^M$ is a *proper class*, that is,

$$\mathrm{On}^M \notin M \tag{1}$$

Indeed, $\mathrm{On}^M$ is a (real) ordinal, for it contains just ordinals and is a transitive *set* (intersection of two transitive classes). If $\mathrm{On}^M \in M$, then $\mathrm{On}^M \in \mathrm{On} \cap M = \mathrm{On}^M$. It also happens to be the *smallest (real) ordinal not in $M$*: If $\alpha < \mathrm{On}^M$, then $\alpha \in \mathrm{On}^M = M \cap \mathrm{On}$.

Similarly, transitivity of $M[G]$ yields that $\mathrm{On}^{M[G]} = M[G] \cap \mathrm{On}$ and that $\mathrm{On}^{M[G]}$ is the smallest ordinal not in $M[G]$. Since, trivially, $\mathrm{On}^M \subseteq \mathrm{On}^{M[G]}$, that is, $\mathrm{On}^M \leq \mathrm{On}^{M[G]}$, we will be done if we can show that

$$\mathrm{On}^M \notin M[G] \tag{2}$$

Well, if (2) is false, then $\mathrm{On}^M = c^G$ for some $c \in M$, and hence (VIII.6.1) $\rho(\mathrm{On}^M) \leq \rho(c)$. Since $(\rho(c) \in \mathrm{On})^M$ is true (why?), we have $\rho(c)^M \in \mathrm{On}^M$, that is, $\rho(c) < \mathrm{On}^M$ (absoluteness of $\rho$), a contradiction (from $\rho(\mathrm{On}^M) = \mathrm{On}^M + 1$ – cf. VI.6.21). □

**VIII.6.3 Remark.** By absoluteness of $\omega$ and of natural numbers, $n \in \mathrm{On}$ and $\omega \in \mathrm{On}$ relativize (for any transitive class $\mathfrak{M}$) to $n \in \mathrm{On}^{\mathfrak{M}}$ and $\omega \in \mathrm{On}^{\mathfrak{M}}$ respectively. In particular, $0, 1, 2, \ldots, \omega$ are in both $M$ and $M[G]$. □

**VIII.6.4 Theorem.** *The $M[G]$-relativizations of the* ZFC *axioms are true.*

*Proof.*

(i) Urelement axioms:

(a) Urelements are atomic: Let $y \in M[G]$. We want the truth of $\big(U(y) \rightarrow \neg(\exists x)x \in y\big)^{M[G]}$. That is, of $U(y) \rightarrow \neg(\exists x \in M[G])x \in y$, which is true even without the qualification $(\exists x)(x \in M[G] \wedge \cdots)$.

(b) Set of all atoms: We want $\{x : U(x)\}^{M[G]} \in M[G]$. That is, $\big(M[G] \cap \{x : U(x)\}\big) \in M[G]$. This is so by VIII.2.9 – whence $M[G] \cap \{x : U(x)\} = M \cap \{x : U(x)\}$ – along with $M \subseteq M[G]$ and the fact that $M$ is a CTM, so that $\{x : U(x)\}^M \in M$.

(ii) Extensionality: It holds because $M[G]$ is transitive (VI.8.10).

(iii) Separation: Let $a \in M$ and $b = \{x \in a^G : \mathscr{A}^{M[G]}(x)\}$, where $\mathscr{A}(x)$ is over $L_{\mathrm{Set},M}$. We let

$$c = \{\langle x, p\rangle \in \mathrm{dom}(a) \times |\mathfrak{P}| : p \Vdash^{w} x \in a \wedge \mathscr{A}(x)\} \tag{1}$$

[†] Not relativized.

By VIII.3.4, the condition to the right of ":" is equivalent to a formula relativized to $M$. Moreover, $\mathrm{dom}(a) \times |\mathfrak{P}| \in M$, since $M$ is a CTM of ZFC. Thus $c \in M$. We now verify that $b = c^G$, and we are done. Indeed:

$\supseteq$: Let $z \in c^G$. Then $z = x^G$ for some $x$ satisfying $\langle x, p\rangle \in c$, for some $p \in G$. Then (1) yields that $x \in \mathrm{dom}(a)$ and that $x^G \in a^G \wedge \mathscr{A}^{M[G]}(x^G)$ is true by VIII.3.5. This says $x^G \in b$.

$\subseteq$: Let $z \in b$. Then $z \in a^G$; therefore $z = x^G$ for some $x \in \mathrm{dom}(a)$. The second part of the entrance requirement in $b$ yields the truth of $\mathscr{A}^{M[G]}(x^G)$. Thus, $x \in \mathrm{dom}(a) \wedge x^G \in a^G \wedge \mathscr{A}^{M[G]}(x^G)$ is true. By VIII.3.5, $x \in \mathrm{dom}(a) \wedge p \Vdash^w x \in a \wedge \mathscr{A}(x)$ is true for some $p \in G \subseteq |\mathfrak{P}|$. Thus, $\langle x, p\rangle \in c$ by (1). But then $x \in_G c$; hence $x^G \in c^G$.

The case with parameters, $\mathscr{A}(x, \vec{y})$, presents no additional difficulties.

(iv) Pairing: By VIII.2.10.

(v) Union: We want to prove that for any $a^G \in M[G]$ a set $b^G \in M[G]$ exists such that ($\bigcup$ is absolute for transitive classes – cf. Section VI.8)

$$\bigcup a^G \subseteq b^G$$

We concentrate on the case where $\neg U(a^G)$, for otherwise the result is trivial by absoluteness of $\emptyset$ for transitive classes (take $b^G = \emptyset$).

Now, analyzing the issue inside $\mathbb{U}_A$, we find that

$$\bigcup a^G = \{x^G : (\exists y \in \mathrm{dom}(a)) x^G \in y^G\} \tag{2}$$

But then, taking $b = \bigcup \mathrm{dom}(a)$ is what we want: Indeed, first, as $M$ is a CTM for ZFC, and $\bigcup$ and dom are absolute, we have $b \in M$; hence $b^G \in M[G]$. Moreover, by (2), if $z \in \bigcup a^G$, then $z$ has the form $x^G$ where, for some $y \in \mathrm{dom}(a)$, $x \in_G y$. Say $\langle x, p\rangle \in y$ for some $p \in |\mathfrak{P}|$. Thus $\langle x, p\rangle \in b$; hence $x^G \in b^G$.

(vi) Foundation: Holds in any class (VI.8.11).

(vii) Collection: Again we look into the parameterless situation. Suppose that we know that

$$(\forall x \in a^G)(\exists y \in M[G])\mathscr{A}^{M[G]}(x, y) \text{ is true} \tag{3}$$

where $\mathscr{A}$ is over $L_{\mathrm{Set},M}$ and $a \in M$. We want to show that a set $b \in M$ exists such that

$$(\forall x \in a^G)(\exists y \in b^G)\mathscr{A}^{M[G]}(x, y) \text{ is true} \tag{4}$$

Since collection is true in $M$, the following holds in $M$ (we have implicitly invoked VIII.3.4 to obtain a formula, relativized to $M$, equivalent to

"$p \Vdash^w \mathscr{A}(z, u)$"):

$$(\forall \langle z, p\rangle \in \mathrm{dom}(a) \times |\mathfrak{P}|)(\exists u \in M)\Big(p \Vdash^w \mathscr{A}(z, u)\Big) \\ \to (\exists W \in M)(\forall \langle z, p\rangle \in \mathrm{dom}(a) \times |\mathfrak{P}|)(\exists u \in W) p \Vdash^w \mathscr{A}(z, u)$$

Or, moving $(\exists W)$ to the front and asserting it to be a set (permissible by III.8.4),

there is a set $W$ in $M$ such that

$$(\forall \langle z, p\rangle \in \mathrm{dom}(a) \times |\mathfrak{P}|)(\exists u \in M)\Big(p \Vdash^w \mathscr{A}(z, u)\Big) \\ \to (\forall \langle z, p\rangle \in \mathrm{dom}(a) \times |\mathfrak{P}|)(\exists u \in W) p \Vdash^w \mathscr{A}(z, u) \tag{5}$$

Now fix a $W \in M$ that verifies (5), and let $b = W \times \{1\}$. Clearly, by closure of $M$ under $\times$ and pairs, $b \in M$. We will show that $b^G$ works for (4). First off, an easy calculation (similar to that in the proof of VIII.2.8) gives

$$b^G = \{y^G : y \in W\} \tag{6}$$

Towards (4), let $x \in a^G$. Then $x = v^G$ for some $v \in M$ and, moreover, $v \in_G a$. Therefore

$$v \in \mathrm{dom}(a) \tag{7}$$

By (3) fix a $y \in M[G]$ that makes $\mathscr{A}^{M[G]}(v^G, y)$ true. Since $y = t^G$ for some $t \in M$, we have the truth of $\mathscr{A}^{M[G]}(v^G, t^G)$; hence, for said $v$ and $t$, and some $p \in G$ (by VIII.3.5),

$$p \Vdash^w \mathscr{A}(v, t) \tag{8}$$

By (7) and (8), using $z = v$ and $u = t$ in (5), we have satisfied an instance of the hypothesis of (5). Thus, there is some $c \in W$ such that $p \Vdash^w \mathscr{A}(v, c)$. By the truth lemma (recall that the $p$ we are talking about is in $G$),

$$\mathscr{A}^{M[G]}(v^G, c^G) \text{ is true}$$

Moreover, $c^G \in b^G$ by (6). Thus $c^G$ will do as an instance of $y$ in (4).

(viii) Power set: Let $a \in M$. We want to show that for some $b \in M$,

$$\{x \in M[G] : x \subseteq a^G\} \subseteq b^G \tag{9}$$

It will turn out that $b = \mathbf{P}(\mathrm{dom}(a) \times |\mathfrak{P}|)^M \times \{1\}$ works. First off, since $M$ satisfies ZFC, $b \in M$. The same type of calculation we have done in the collection case yields

$$b^G = \{z^G : z \in \mathbf{P}(\mathrm{dom}(a) \times |\mathfrak{P}|)^M\} \tag{10}$$

Let now $x \in M[G] \wedge x \subseteq a^G$. We show that $x \in b^G$. By hypothesis, $x = c^G$ for some $c \in M$. We form

$$d = \{\langle z, p\rangle \in \mathrm{dom}(a) \times |\mathfrak{P}| : p \Vdash^w z \in c\} \tag{11}$$

By VIII.3.4, $d \in M$, since separation is true in $M$. We now see that $d$ is a "better" name for $x$ above – i.e., for $c^G$ – than $c$ is, because, using the name $d$, it is easy to show that $d^G \in b^G$. We have two claims here: First, $c^G = d^G$.

$\subseteq$: Let $y \in c^G$. Then $y = z^G$ for some $z \in \mathrm{dom}(a)$ (recall that $c^G \subseteq a^G$). By the truth lemma, there is a $p \in G$ such that $p \Vdash^w z \in c$; hence, by (11), $\langle z, p\rangle \in d$. Hence, $z^G \in d^G$ (for $z \in_G d$).

$\supseteq$: Let $y \in d^G$. Then $y = z^G$ for some $z \in M$, and there is a $p \in G$ such that $\langle z, p\rangle \in d$. By (11), $z \in \mathrm{dom}(a)$ and $p \Vdash^w z \in c$. Remembering that $p \in G$, we get $z^G \in c^G$ by VIII.3.5.

Second, we show that $d^G \in b^G$, which concludes our task. But this is so by (10), since $d \in \mathbf{P}(\mathrm{dom}(a) \times |\mathfrak{P}|)^M$.

(ix) Infinity: $\omega \in M \subseteq M[G]$.

(x) AC: It is convenient to use the version of AC given by Corollary VI.5.53. Fix then a set $x \in M[G]$. For some set $a \in M$, $x = a^G$. By the corollary, let $f = \{\langle \beta, f(\beta)\rangle : \beta \in \alpha\}$ in $M$ such that $\mathrm{dom}(a) \subseteq \mathrm{ran}(f)$ – possible by AC$^M$. Recalling VIII.2.10 and VIII.2.6, we let

$$F = \Big\{\big\{\hat{\beta}, \{\hat{\beta}, f(\beta)\} \times \{1\}\big\} \times \{1\} : \beta \in \alpha\Big\} \times \{1\} \tag{12}$$

Now $F \in M$. What is $F^G$? Using VIII.2.10 and VIII.2.6, we calculate (as we did to obtain (6) above)

$$\begin{aligned} F^G &= \Big\{\big(\big\{\hat{\beta}, \{\hat{\beta}, f(\beta)\} \times \{1\}\big\} \times \{1\}\big)^G : \beta \in \alpha\Big\} \\ &= \Big\{\big\{\beta, \{\beta, f(\beta)^G\}\big\} : \beta \in \alpha\Big\} \\ &= \Big\{\big\langle \beta, f(\beta)^G\big\rangle : \beta \in \alpha\Big\} \end{aligned}$$

Thus $F^G$ is a function in $M[G]$ with domain $\alpha$ (VIII.6.2). If $y^G \in a^G$, then $y \in \mathrm{dom}(a)$; hence $y = f(\beta)$ for some $\beta \in \alpha$ by choice of $f$, and therefore $y^G = f(\beta)^G$. Thus $a^G \subseteq \mathrm{ran}(F^G)$. □

We have been repetitiously insisting throughout this chapter that a being in $M$ be empowered to "force things to happen" in $M[G]$ for any $M$-generic $G$. The proof of the above theorem clarifies the meaning of that intention and shows that it is wise and feasible: A being in $M$ knows that ZFC is true in $M$. We have ensured that he can use this knowledge and the $p \Vdash^w \ldots$ construct, which is expressible in $M$, to force the truth of the ZFC axioms in a world ($M[G]$) that, for him, is "imaginary" or unreachable.

Actually he can do more, and this is the subject of the next section: By choosing the notion of forcing $\mathfrak{P}$ in $M$ appropriately, he can force all sorts of weird things to happen in the imaginary world $M[G]$, such as $2^{\aleph_0} = \aleph_{\aleph_1}$. And, of course, he can force the truth of $\neg$CH.

Finally, we note that the name "generic" for the sets $G$ (for any fixed $\mathfrak{P}$) is apt. They all "code the same information", i.e., it does not matter which particular $M$-generic $G \subseteq |\mathfrak{P}|$ we choose. If $M$ is a CTM for ZFC, then $M[G]$ is a CTM for ZFC. Moreover, if a $\mathfrak{P}$ forces some additional properties (such as $\neg$CH) to be true in $M[G]$, this is so for *any* $M$-generic $G \subseteq |\mathfrak{P}|$.

## VIII.7. Applications

We conclude our lectures by presenting in this section elementary applications of forcing. They all are based on PO sets of finite functions. We recall from Section VI.8 that finiteness is absolute for CTMs of ZFC and therefore an inhabitant of such a CTM proclaims a set "finite" exactly when such a set is "really" finite. We will benefit from widening the scope of Examples VIII.1.3, VIII.1.6, and VIII.1.9.

**VIII.7.1 Example.** Let[†] $\mathfrak{F}(a, b) = \langle F(a, b), <, 1\rangle$ be a PO set defined as follows in terms of sets $a$ and $b$ where $a$ is infinite and $b \neq \emptyset$:[‡]

$$F(a, b) = \{p \mid p : a \rightharpoonup b \text{ is a finite function}\}$$

1 is the function $\emptyset : a \rightharpoonup b$ with empty domain. $p < q$ will mean $p \supset q$ (reverse inclusion). Let $M$ be a CTM and $\mathfrak{F} \in M$. Then absoluteness of pairing and finiteness allows the preceding definition to take place inside $M$ with the same result as if it were effected in $\mathbb{U}_A$. Let $G \subseteq F$ be $M$-generic. Then $f = \bigcup G$ is a function $a \rightarrow b$ that is total and onto. That it is a function follows from the compatibility of $p$ and $q$ in $G$ as in VIII.1.9. For totalness one observes (as in VIII.1.9) that the set $D_i = \{p \in F : p(i)\downarrow\}$ is dense in $M$ for all $i \in a$. For ontoness we employ the dense sets $R_i$, for $i \in b$, where $R_i = \{p \in F : i \in \operatorname{ran}(p)\}$. Indeed, let $q \in F$. If $q(i)\downarrow$, then $q \in D_i$. Otherwise,

$$D_i \ni q \cup \{\langle i, j\rangle\} < q$$

[†] No connection between this "$\mathfrak{F}$" and Gödel operations of Section VI.9.

[‡] We have used "$\{p \mid \ldots\}$" rather than our usual "$\{p : \ldots\}$" because a "$p : a \ldots$" follows a few symbols away.

where we have picked $j \in b$ arbitrarily ($b \neq \emptyset$). Similarly, if $i \in \mathrm{ran}(q)$, then $q \in R_i$, else

$$R_i \ni q \cup \{\langle j, i\rangle\} < q$$

where we have picked $j \in a - \mathrm{dom}(q)$ ($a$ is infinite in $M$).

Thus, $G \cap D_i \neq \emptyset \neq G \cap R_j$ for all $i \in a$ and all $j \in b$. That is, for all these $i$, $j$ there are finite subfunctions of $f$ – $p$ and $q$ – with $p(i) \downarrow$ and $j \in \mathrm{ran}(q)$. That is, we have verified totalness and ontoness.

As in VIII.1.9, $G \notin M$ if $b$ has two or more elements. Indeed, under the present circumstances, if $G \in M$, then so is $F - G$, and we get a contradiction as follows: First, $F - G$ is dense. Indeed, let $q \in F$. Pick $i \in a - \mathrm{dom}(q)$ and $j, m$ distinct members of $b$. Then

$$q \cup \{\langle i, j\rangle\} \perp q \cup \{\langle i, m\rangle\}$$

Thus one of these extensions of $q$ must be in $F - G$. Having verified the density of this latter set, we now have $(F - G) \cap G \neq \emptyset$.

It is useful to rephrase the fact that $G \notin M$: $M \subset M[G]$. □

Absoluteness results of Sections VI.8 and VI.9 (in particular VI.9.20) show that the function $\alpha \mapsto F_\alpha$ of VI.9.2 is absolute for any CTM of ZF as long as we take $N$ of $\mathbb{L}_N$ in $M$. Thus, if $M$ is such a CTM, then

$$\mathbb{L}_N^M = \{F_\alpha : \alpha \in \mathrm{On}\}^M = \{F_\alpha : \alpha \in \mathrm{On}^M\} \tag{1}$$

If now $M$ is a CTM of ZFC and we take $a = \omega$ and $b = 2$ in Example VIII.7.1, we have, for any $M$-generic $G$, that $M[G]$ is a CTM of ZFC (Theorem VIII.6.4) and, moreover,

$$\mathbb{L}_N^{M[G]} = \{F_\alpha : \alpha \in \mathrm{On}\}^{M[G]} = \{F_\alpha : \alpha \in \mathrm{On}^{M[G]}\} \tag{2}$$

Since $\mathrm{On}^M = \mathrm{On}^{M[G]}$ (by VIII.6.2), (1) and (2) yield

$$\mathbb{L}_N^M = \mathbb{L}_N^{M[G]}$$

or, in words, $M$ and $M[G]$ have the same constructible sets.

Now, by the conclusion of the preceding example and in view of what we have just remarked, any $x \in M[G] - M$ is a *set* ($M$ and $M[G]$ have the same atoms; cf. VIII.2.9) that is *not constructible in* $M[G]$. Thus, on the assumption that $M$ is a model of ZFC, we now have a model of ZFC + ($\mathbb{V} \neq \mathbb{L}$), namely $M[G]$. More specifically, it turns out that not only $G \notin M$, but also $\bigcup G \notin M$ (see Exercise VIII.2). This function – viewed as a characteristic function – defines a subset of $\omega$. This subset is not in $M$, and hence is not constructible in $M[G]$. For the record we state all this as follows:

**VIII.7.2 Proposition (Cohen).** *It is consistent with* ZFC *that non-constructible sets exist. In fact, it is consistent with* ZFC *that a non-constructible subset of* $\omega$ *exists.*

**VIII.7.3 Example (Collapsing Cardinals).** Once more we look at Example VIII.7.1. This time we fix a CTM of ZFC, $M$, and take $a = \omega$ and $b = \aleph_1^M$.

Of course, $\aleph_1^M$ is the smallest ordinal $\alpha > \omega$ in $M$ for which there is no 1-1 correspondence $f : \omega \to \alpha$ $\underline{\text{in } M}$.

Let $G$ be $M$-generic with respect to the PO set $\mathfrak{F}(\omega, \aleph_1^M)$, and consider $g = \bigcup G$. We know that $g \in M[G]$. We also know that $g : \omega \to \alpha$ is total and onto in $M[G]$ (recall that ordinals are absolute, and $M$ and $M[G]$ have the same ordinals). Thus, $\alpha$ is *not* an uncountable *cardinal* $\underline{\text{in } M[G]}$; it is just an at most countable ordinal (in view of $g$). We say that the cardinal $\aleph_1^M$ was *collapsed* as we passed from $M$ to its generic extension $M[G]$. Therefore $\aleph_1^M$ is not an uncountable cardinal in $M[G]$, that is, $\aleph_1^M < \aleph_1^{M[G]}$ in $M[G]$. Of course, all along, $\aleph_1^M$ is just that $\alpha$ above.

This phenomenon of cardinals collapsing – a witness to the fact that being a cardinal is not absolute for CTMs – is annoying because it causes more work towards proving the relative consistency of $\neg$CH. □

Of course, at most countable cardinals do not collapse, by absoluteness of $\omega$ and of finite ordinals. Moreover, going backwards, all cardinals are preserved.

**VIII.7.4 Proposition.** *Let* $\alpha$ *be an ordinal in* $M[G]$ *such that* ($\alpha$ *is a cardinal*)$^{M[G]}$. *Then* ($\alpha$ *is a cardinal*)$^M$.

*Proof.* $\alpha$ is an ordinal in $M$ by VIII.6.2. Suppose that the conclusion is false, and let $\beta < \alpha$ and $f : \beta \to \alpha$ be a 1-1 correspondence in $M$. Now "$f$ is a 1-1 correspondence" is absolute for transitive models of ZF, and $\beta$ and $f$ are in $M[G]$. This contradicts that $\alpha$ is a cardinal in $M[G]$. □

**VIII.7.5 Example (Towards the Relative Consistency of $\neg$CH).** We turn once again to Example VIII.7.1. This time we fix a CTM of ZFC, $M$, and take an $\mathfrak{F}(a, b) \in M$ with $a = \omega \times \kappa$ and $b = 2$, where $\kappa$ is an uncountable cardinal in $M$, or

$$(\kappa \text{ is an uncountable cardinal})^M \tag{1}$$

Let $G$ be $M$-generic and form $M[G]$. We know that if we let $f = \bigcup G$, then

$$f : \omega \times \kappa \to 2 \text{ is total and onto} \tag{2}$$

and

$$f \notin M \qquad \text{by Exercise VIII.2} \tag{3}$$

As a matter of fact, $\alpha \mapsto \lambda n.f(n, \alpha)$[†] is 1-1 on $\kappa$: Indeed, for any $\alpha \neq \beta$ in $\kappa$ consider the set in $M$,

$$D = \Big\{p \in F(\omega \times \kappa, 2) : (\exists n \in \omega)\big(p(n, \alpha) \downarrow \wedge \\ p(n, \beta) \downarrow \wedge p(n, \alpha) \neq p(n, \beta)\big)\Big\}$$

$D$ is dense, as we can extend any $q \in F(\omega \times \kappa, 2)$ by adding the triples $\langle\langle n, \alpha\rangle, 0\rangle$ and $\langle\langle n, \beta\rangle, 1\rangle$ to $q$, for some $n$ such that $q(n, \alpha) \uparrow$ and $q(n, \beta) \uparrow$ (there are plenty of such $n$, by finiteness of $q$). Now $G \cap D \neq \emptyset$ translates to $f(n, \alpha) \neq f(n, \beta)$ for some $n \in \omega$; hence $\lambda n.f(n, \alpha) \neq \lambda n.f(n, \beta)$.

Since the function $f$ is in $M[G]$, so is $\alpha \mapsto \lambda n.f(n, \alpha)$. The latter being 1-1 and total (on $\kappa$), it establishes

$$\Big(\mathrm{Card}({}^{\omega}2) \geq \mathrm{Card}(\kappa)\Big)^{M[G]} \tag{4}$$

or

$$(2^{\aleph_0})^{M[G]} \geq \mathrm{Card}^{M[G]}(\kappa) \tag{5}$$

Of course, the *ordinal* $\kappa$ is an ordinal to inhabitants of both worlds, $M$ and $M[G]$, but it would be reckless to assume, *a priori*, that $\kappa$ is a cardinal in $M[G]$ just by virtue of being so in $M$ – after all, we saw that cardinals *may* collapse. Hence our conservatism in using "$\mathrm{Card}^{M[G]}(\kappa)$" rather than just "$\kappa$" in (4) and (5) above.

Now, outside the context of a CTM, to deny CH (that says $2^{\aleph_0} = \aleph_1$) is to manage to get $2^{\aleph_0} > \aleph_1$, in other words

$$2^{\aleph_0} \geq \aleph_2$$

In view of (5) and the above (relativized to $M[G]$) it would then suffice to take $\kappa = \aleph_2^M$ and prove that uncountable cardinals, at least the two particular ones $\aleph_1^M$ and $\aleph_2^M$, are *preserved* as we pass from $M$ to a generic extension (with

[†] Or $\lambda\alpha.(\lambda n.f(n, \alpha))$.

respect to the present $\mathfrak{F}(a, b)$) $M[G]$, that is, we would like to show $\aleph_1^M = \aleph_1^{M[G]}$ and $\aleph_2^M = \aleph_2^{M[G]}$.

We will do that through a sequence of lemmata.

**Pause.** If $\aleph_2^M$ collapses, then we are in trouble: (5) does nothing for us, because the *ordinal* $\aleph_2^M$ is countable in $M[G]$. If $\aleph_1^M$ collapses, even if $\aleph_2^M$ might not, we are still in trouble, for $\aleph_2^M$ is *not* the second infinite cardinal in $M[G]$ (that is, $\aleph_2^{M[G]}$) now that $\aleph_1^M$ has collapsed. □

**VIII.7.6 Remark.** Since for each $\alpha < \kappa$, $\lambda n.f(n, \alpha)$ codes a real number in $[0, 1]$ (in binary notation), we say that $\lambda n.f(n, \alpha)$ is a *Cohen generic real*. Thus we have added (these objects are new, by Exercise VIII.2) $\kappa$ generic reals to the ground model $M$. Intuitively, this set of reals turns out to be so huge that, *in* $M[G]$, it has cardinality large enough to allow some cardinalities below it, but above $\omega$. □

**VIII.7.7 Definition (The $\kappa$-Antichain Condition).** Let $\kappa$ be an infinite cardinal. A PO set $\mathfrak{P} = \langle P, <, 1\rangle$ has the *$\kappa$-antichain condition*, for short $\kappa$-a.c., if every antichain $A \subseteq P$ has cardinality $< \kappa$. □

In much of the literature the $\kappa$-antichain condition is called the *$\kappa$-chain* condition or $\kappa$-c.c. In particular, when $\kappa = \aleph_1$ one then speaks of the *countable chain condition* or c.c.c.

**VIII.7.8 Lemma.** *Let $M$ be a CTM of* ZFC, *and $\mathfrak{P} = \langle P, <, 1\rangle$ a PO set in $M$ that has $\kappa$-a.c. in $M$.*[†] *Assume that $\kappa$ is a regular uncountable cardinal in $M$ – that is, $\big(\omega < \kappa \wedge \kappa$ is regular$\big)^M$ holds. Then $\kappa$ is also a cardinal in $M[G]$ for any $M$-generic $G \subseteq P$.*

*Proof.* Suppose instead that hypotheses hold, yet there is an $M$-generic $G$ and an onto function in $M[G]$, $f : \alpha \to \kappa$, where $\alpha < \kappa$ in $M[G]$. That is, the ordinal $\kappa$ is not a cardinal in $M[G]$. By VIII.6.2, $\alpha$ is an ordinal in $M$ as well.

There is a formula $\mathscr{A}(x, y, z)$ of $L_{\text{Set}}$ that says "$x : y \to z$ is an onto function". Thus, if $t \in M$ is such that $f = t^G$, then, for some $p \in G$ (we fix one such $p$), VIII.3.5 implies

$$p \Vdash^w \mathscr{A}(t, \hat{\alpha}, \hat{\kappa})$$

[†] The "in $M$" cannot be emphasized enough. Since $M$ is countable, a resident of $\mathbb{U}_A$ trivially sees that every antichain in $M$ is countable.

In words, we have the following sentence true in $M$:

$$p \Vdash^w t : \hat{\alpha} \to \hat{\kappa} \text{ is onto} \tag{1}$$

where the ˆ-function is that of VIII.2.6.

For every $\beta < \alpha$ we let

$$B_\beta = \{\gamma < \kappa : (\exists q \leq p) q \Vdash^w t(\hat{\beta}) = \hat{\gamma}\} \tag{2}$$

$B_\beta \in M$ for all $\beta < \alpha$, since, by the definability lemma, the expression to the right of ":" is a formula relativized to $M$. We next majorize the cardinality in $M$ of the $B_\beta$, i.e., estimate ("from above") $\text{Card}^M(B_\beta)$. To this end, let us pick for each $\gamma \in B_\beta$ *one* $q$ that works in (2) above. We denote this $q$ by $q_\gamma$.

Assume now that $\gamma \neq \delta$ are both in $B_\beta$. We will argue that $q_\gamma \perp q_\delta$: If not, let $r \leq q_\gamma$ and $r \leq q_\delta$. Now, by definition of the symbol "$q_\gamma$", $q_\gamma \Vdash^w t(\hat{\beta}) = \hat{\gamma}$ and $q_\delta \Vdash^w t(\hat{\beta}) = \hat{\delta}$; hence, by monotonicity (VIII.3.3(2)), $r \Vdash^w t(\hat{\beta}) = \hat{\gamma}$ and $r \Vdash^w t(\hat{\beta}) = \hat{\delta}$. Let $G' \ni r$ be some $M$-generic set (cf. VIII.1.8). The truth lemma yields $\gamma = t^{G'}(\beta) = \delta$ in $M[G']$ (recall that ordinals are preserved, and both $\gamma$ and $\delta$ are in $M$, for $\kappa$ is). This is a contradiction.

**Pause.** While $G' \neq G$ in $\mathbb{U}_A$ in general, and the same is true of $t^{G'}$ versus $t^G = f$, these objects – $G'$ and $t^{G'}$ – were just intermediate agents towards deriving the contradiction $\gamma = \delta$.

Thus, in $M$, $B_\beta$ maps 1-1 into some antichain $C$ that contains the $q_\gamma$ objects for the various $\gamma \in B_\beta$. Therefore, $\text{Card}(B_\beta) \leq \text{Card}(C) < \kappa$ is true in $M$,[†] the "<" contributed by the $\kappa$-a.c. of $\mathfrak{P}$ in $M$. Since $\kappa$ is regular in $M$, the following is true in $M$ by VII.6.11:

$$\text{Card}\Big(\bigcup_{\beta<\alpha} B_\beta\Big) < \kappa \tag{3}$$

We will next contradict (3) by proving, in $M$,

$$\kappa \subseteq \bigcup_{\beta<\alpha} B_\beta \tag{4}$$

This shows that the assumption that we have an $\alpha$ and $f$ in $M[G]$ with the stated properties is untenable, thus proving the lemma.

Towards (4), let us argue in $M$, and let $\gamma < \kappa$ (i.e., $\gamma \in \kappa$). Since $f$ is onto $\kappa$ (from $\alpha$ – this happens in $M[G]$), let $\beta < \alpha$ such that $f(\beta) = \gamma$. Thus, by

[†] Written without the $M$-superscript, since we have said "is true in $M$" (cf. VI.8.4).

the truth lemma, some $q \in G$ satisfies

$$q \Vdash^w t(\hat{\beta}) = \hat{\gamma} \tag{5}$$

We will be done if we can say "without loss of generality, $q \leq p$" for the $p$ we have fixed at the outset of our proof (cf. (1)), for then $\gamma \in B_\beta$ by (2). To settle the phrase in quotes, let $r \in G$ be such that $r \leq q$ and $r \leq p$ – it exists because both $q$ and $p$ are in $G$. Then $r \Vdash^w t(\hat{\beta}) = \hat{\gamma}$ by monotonicity (and the fact that $q$ works). □

**VIII.7.9 Definition.** Let $M$ be a CTM of ZFC, and $\mathfrak{P} = \langle P, <, 1\rangle$ a PO set in $M$. We say that $\mathfrak{P}$ *preserves cardinals* just in case for every $M$-generic $G \subseteq P$ and every ordinal $\alpha$ of $M$ (i.e., $\alpha \in \mathrm{On}^M$), if $\alpha$ is a cardinal in $M$, then it is also a cardinal in $M[G]$. □

By absoluteness of $\omega$ and below, finite or countable cardinals are always preserved (forward, from $M$ to $M[G]$). By VIII.7.4 cardinals are also preserved backwards.

Now, Lemma VIII.7.8 gives a sufficient condition for the preservation of all *regular* cardinals (in $M$) above $\kappa$ (clearly, if $\mathfrak{P}$ has the $\kappa$-a.c. in $M$, it also has the $\lambda$-a.c. in $M$ for all cardinals $\lambda > \kappa$). The following strengthens all this a bit, by dropping the qualification *regular*.

**VIII.7.10 Corollary.** *Let $M$ be a CTM of* ZFC*, and $\mathfrak{P} = \langle P, <, 1\rangle$ a PO set in $M$ that has the $\aleph_1$-a.c. in $M$. Then $\mathfrak{P}$ preserves cardinals.*

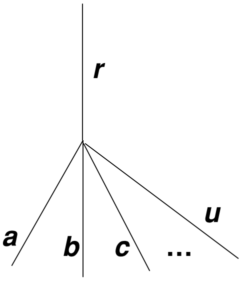
*Proof.* We only worry about what happens beyond $\omega$. By the remarks above, if $\kappa = \aleph^M_{\alpha+1}$, a *successor cardinal*, then $\kappa$ is preserved, since it is regular in $M$ (see VII.6.12). Suppose now that $\kappa = \aleph^M_\alpha$ and $\mathrm{Lim}(\alpha)$, that is, a *limit cardinal*.[†] Thus $\kappa = \bigcup_{\beta<\alpha} \aleph^M_\beta$. By Remark VII.4.24(2), $\kappa = \bigcup_{\beta<\alpha} \aleph^M_{\beta+1}$ and all $\aleph^M_{\beta+1}$ are preserved. □

Our next task is to show that the particular PO set of Example VIII.7.5 has the $\aleph_1$-a.c. (or c.c.c. in the alternative terminology). We will need a definition and two more lemmata.

**VIII.7.11 Definition ($\Delta$-Systems).** A family of sets $A$ is called a $\Delta$*-system*, or a *quasi-disjoint family*, provided that there is a set $r$, the *root* of $A$, such that for any two $a \neq b$ in $A$, $a \cap b = r$. □

[†] $\mathrm{Lim}(\alpha)$ is absolute for CTMs.

The name "Δ-system" is suggested by the shape of a quasi-disjoint family as sketched below (the members of the family depicted below are $r \cup a$, $r \cup b$, $r \cup c$, etc.):



**VIII.7.12 Lemma (Δ-System Lemma).** *If the set $A$ is an uncountable family of finite sets, then there is an uncountable $B \subseteq A$ that is a Δ-system.*

*Proof.* This is argued in ZFC (or in $\mathbb{U}_A$).

First off, for each $n \in \omega$, let $C_n = \{X \in A : \mathrm{Card}(X) = n\}$. There must be an $n \in \omega$ such that $C_n$ is uncountable; otherwise $\mathrm{Card}(A) \le \aleph_0$, since $A = \bigcup_{n\in\omega} C_n$ (this uses AC; see VII.2.13). Thus, without loss of generality, we assume that there is some fixed $n \in \omega$ such that, for all $X \in A$, $\mathrm{Card}(X) = n$.[†] Let us then prove the lemma by induction on $n$.

For the basis, $n = 1$, it suffices to take $B = A$ and $r = \emptyset$.

We proceed to the $n + 1$ case, based on the obvious I.H.

*Case 1.* There is an $a$ such that $S = \{X \in A : a \in X\}$ is uncountable. By the I.H., let $D$ be an uncountable quasi-disjoint subfamily of $\{X - \{a\} : X \in S\}$ with root $r$. Then $B = \{X \cup \{a\} : X \in D\}$ with root $r \cup \{a\}$ is what we want.

*Case 2.* There is no such $a$ as above. We then define by recursion (on ordinals $< \aleph_1$) a transfinite sequence in $A$:

$$\begin{aligned} X_0 &= \text{ some arbitrary set in } A \\ X_\alpha &= \text{ some arbitrary set in } A \text{ that is disjoint from } \bigcup_{\beta<\alpha} X_\beta \end{aligned}$$

Assuming that the recursion above is legitimate, then $\{X_\alpha : \alpha < \aleph_1\}$ is uncountable and quasi-disjoint. Indeed, the $X_\alpha$ are pairwise disjoint, so that $r = \emptyset$ works.

[†] That is, we work with an uncountable $C_n$, call it "$A$", and discard the original $A$.

But why is the second step in the recursion possible for any $\alpha < \aleph_1$? The set $\mathscr{Y} = \big\{Y \in A : Y \notin \{X_\beta : \beta < \alpha\}\big\}$ is uncountable; otherwise

$$\begin{aligned} \mathrm{Card}(A) &\le \aleph_0 (\text{that is, } \mathrm{Card}(\mathscr{Y})) +_c \mathrm{Card}\{X_\beta : \beta < \alpha\} \\ &= \aleph_0 +_c \mathrm{Card}(\alpha) \qquad \text{since } \beta \mapsto X_\beta \text{ is 1-1 and total on } \alpha \\ &= \aleph_0 +_c \aleph_0 \qquad \text{by } \mathrm{Card}(\alpha) \le \alpha < \aleph_1 \\ &= \aleph_0 \end{aligned}$$

We will be done if we can argue that at least one $Y \in \mathscr{Y}$ is disjoint from all $X_\beta$, $\beta < \alpha$. Any such $Y$ can then be chosen to be $X_\alpha$.

Suppose instead that every $Y \in \mathscr{Y}$ intersects $\bigcup_{\beta<\alpha} X_\beta$. Then there is a $\beta_0 < \alpha$ such that $X_{\beta_0} \cap Y \neq \emptyset$ for uncountably many among the $Y \in \mathscr{Y}$ – otherwise, $\mathscr{Y}$ is a countable union of countable sets $\mathscr{Z}_\beta = \{Y \in \mathscr{Y} : X_\beta \cap Y \neq \emptyset\}$, for $\beta < \alpha$. Fixing attention on that $\beta_0$, we prove that some $a \in X_{\beta_0}$ is in uncountably many $Y$, contradicting the case we are arguing under. Well, if not, let for each $a \in X_{\beta_0}$

$$\mathscr{W}_a = \{Y \in \mathscr{Y} : a \in Y\}$$

Each $\mathscr{W}_a$ is countable; hence ($X_{\beta_0}$ being finite) so is $\bigcup_{a \in X_{\beta_0}} \mathscr{W}_a$. But this union is the set of $\mathscr{Y}$-sets that $X_{\beta_0}$ intersects, and that is uncountable. □

By the concluding remarks of Example VIII.7.5, all that remains to be done is the following lemma:

**VIII.7.13 Lemma.** *Let $M$ be a CTM of* ZFC*, and $\mathfrak{F}(a,b) = \langle F(a,b), <, 1\rangle$ a PO set in $M$, where $a = \omega \times \aleph_2^M$ and $b = 2$. Then $\mathfrak{F}(a,b)$ has the $\aleph_1$-a.c. (or c.c.c.) in $M$.*

*Proof.* The argument is carried out inside $M$.

$F(a,b)$ is uncountable. Arguing by contradiction, let $A \subseteq F(a,b)$ be an uncountable antichain. The set

$$B = \{\mathrm{dom}(p) : p \in A\} \tag{1}$$

is also uncountable. If not, $A \subseteq \bigcup_{s\in B}\{p \in F(a,b) : \mathrm{dom}(p) = s\}$, a countable set, since for each finite $s \subseteq \omega \times \aleph_2^M$ the cardinality of ${}^s2$ is finite ($= 2^{\mathrm{Card}(s)}$), and thus $\{p \in F(a,b) : \mathrm{dom}(p) = s\}$ is finite. Let $D \subseteq B$ be an uncountable $\Delta$-system of root $r$, and set $A_D = \{p \in A : \mathrm{dom}(p) \in D\}$. This is uncountable due to the onto map $p \mapsto \mathrm{dom}(p)$.

Now, $\{p\lceil r : p \in A_D\}$ is finite, hence there are plenty of $p$ and $q$ in $A_D$, indeed uncountably many, with $p \neq q$ and $p\lceil r = q\lceil r$. But then $p$ and $q$ are compatible, since $\mathrm{dom}(p)$ and $\mathrm{dom}(q)$ are in $D$, and therefore $\mathrm{dom}(p) \cap \mathrm{dom}(q) = r$. But also $p \perp q$, since both are in $A$. □

For the record, we now have

**VIII.7.14 Corollary (Cohen).** *With $M$ and $\mathfrak{F}(a, b)$ as above, if $G$ is any $M$-generic set, then $(\neg\mathrm{CH})^{M[G]}$ is true.*

Thus, a model of ZFC leads to a model of ZFC $+ \neg$CH.

## VIII.8. Exercises

**VIII.1.** In the definition of generic sets (VIII.1.7) we have required $G$ to be a filter *definitionally*. Prove that in the presence of the density requirement we get that $G$ is a filter for free, relaxing requirement (2) in the definition of a filter (VIII.1.4) as follows: We only ask that any two $p$ and $q$ in $G$ be compatible (without asking for a witness in $G$). (*Hint.* Fix $p$ and $q$ in $G$. It helps to prove that the following set is dense: $\{r \in |\mathfrak{P}| : r \perp p \vee r \perp q \vee (r \leq p \wedge r \leq q)\}$.)

**VIII.2.** Refer to Example VIII.7.1, and take $a = \omega$ and $b = 2$. We have seen that if $M$ is a CTM (of, say, ZF) with $\mathfrak{F}(\omega, 2) \in M$ and $G$ is any $M$-generic set, then $G \notin M$. We also know that $f = \bigcup G$ is a function and $f \in M[G]$. Prove that $f \notin M$.
(*Hint.* Let $g : \omega \to 2$ be in $M$. With the help of the set $\{p \in F(\omega, 2) : (\exists n \in \omega)(p(n) \downarrow \wedge p(n) \neq g(n)\}$, prove that $f \neq g$.)

**VIII.3.** If $M$ is a transitive model of ZF − P, then the following are absolute for $M$, where we write $\pi_i$, $i = 1, 2, 3$, for the $i$th projection of $\langle x, y, z\rangle$:
(a) $\mathbf{P}_\omega(A)$, where $\mathbf{P}_\omega(A) = \{x : x \subseteq A \wedge x \text{ is finite}\}$.
(b) $x$ is a PO set.
(c) $x$ is a PO set $\wedge\, y \in \pi_1(x) \wedge z \in \pi_1(x) \wedge y \perp z$.
(d) $x$ is a PO set $\wedge\, y \subseteq \pi_1(x) \wedge \neg U(y) \wedge y$ is open.
(e) $x$ is a PO set $\wedge\, y \subseteq \pi_1(x) \wedge \neg U(y) \wedge y$ is dense.
(f) $x$ is a PO set $\wedge\, y \subseteq \pi_1(x) \wedge \neg U(y) \wedge \neg U(z) \wedge y$ is $z$-generic.

**VIII.4.** Prove that $\lambda x G.x^G$ is absolute for transitive models of ZF − P.

**VIII.5.** Prove that $\lambda x \mathfrak{P}.\hat{x}$ of VIII.2.6 is absolute for transitive models of ZF − P.

**VIII.6.** Provide all the necessary details that show $\mathbb{I}n$ and $\mathbb{N}e$ are absolute for any transitive model of ZF − P.

**VIII.7.** Chose an $M$, a PO set $\mathfrak{P}$ in $M$, and $G \subseteq M$ (not necessarily generic). Show that $(x \cup y)^G = x^G \cup y^G$ for all $x$ and $y$ in $M$.

**VIII.8.** Simplify the expressions, giving your answer in terms of $\Vdash$ or $\Vdash^w$ (that is, $\models$ should not figure in the final answer).

(a) $p \Vdash^w \neg \mathscr{A}$

(b) $p \Vdash^w \mathscr{A} \vee \mathscr{B}$

(c) $p \Vdash^w (\forall x)\mathscr{A}(x, \vec{y})$

(d) $p \Vdash^w (\exists x)\mathscr{A}(x, \vec{y})$

(e) $p \Vdash \mathscr{A} \wedge \mathscr{B}$

(f) $p \Vdash (\forall x)\mathscr{A}(x, \vec{y})$

**VIII.9.** Let $M$ be a CTM of ZFC, $\mathfrak{P}$ a PO set in $M$, $p \in |\mathfrak{P}|$, and $\mathscr{A}$ a sentence over $L_{\mathrm{Set},M}$. Assume that $D = \{q \in |\mathfrak{P}| : q \Vdash^w \mathscr{A}\}$ is *dense below* $p$, which means that for every $r \leq p$, $(\leq\langle r\rangle) \cap D \neq \emptyset$. Prove that $p \Vdash^w \mathscr{A}$.

**VIII.10.** Given sentences $\mathscr{A}_1, \ldots, \mathscr{A}_n, \mathscr{B}$ over $L_{\mathrm{Set},M}$, for some CTM of ZFC, $M$, and a PO set $\mathfrak{P}$ in $M$. Prove that if we have $\mathscr{A}_1, \ldots, \mathscr{A}_n \vdash_{\mathrm{ZFC}} \mathscr{B}$ and $p \Vdash^w \mathscr{A}_i$ $(i = 1, \ldots, n, p \in |\mathfrak{P}|)$, then we also have $p \Vdash^w \mathscr{B}$.

# Bibliography

Aczel, P. (1978). An introduction to inductive definitions. In Barwise (1978), Chapter C.7, pages 739–782.

Apostol, T. (1957). *Mathematical Analysis*. Addison-Wesley, Reading, Massachusetts.

Bachmann, H. (1955). *Transfinite Zahlen*. Berlin.

Barwise, Jon (1975). *Admissible Sets and Structures*. Springer-Verlag, New York.

——— (1978), editor. *Handbook of Mathematical Logic*. North-Holland, Amsterdam.

——— and L. Moss (1991). Hypersets. *The Mathematical Intelligencer*, 13(4):31–41.

Blum, E. (1967). A machine-independent theory of the complexity of recursive functions. *J. ACM*, 14:322–336.

Bourbaki, N. (1966a). *Éléments de Mathématique*. Hermann, Paris.

——— (1966b). *Éléments de Mathématique; Théorie des Ensembles*. Hermann, Paris.

Burgess, John P. (1978). Forcing. In Barwise (1978), Chapter B.4, pages 403–452.

Cohen, P. J. (1963). The independence of the continuum hypothesis, part I. *Proc. Nat. Acad. Sci. U.S.A.*, 50:1143–1148. Part II, 51:105–110 (1964).

Davis, M. (1965). *The Undecidable*. Raven Press, Hewlett, N.Y.

Dedekind, R. (1888). *Was Sind und Was Sollen die Zahlen?* Vieweg, Braunschweig.

Devlin, K. J. (1978). Constructibility. In Barwise (1978), Chapter B.5, pages 453–489.

Dijkstra, Edsger W., and Carel S. Scholten (1990). *Predicate Calculus and Program Semantics*. Springer-Verlag, New York.

Enderton, Herbert B. (1972). *A Mathematical Introduction to Logic*. Academic Press, New York.

Feferman, S. (1965). Some applications of the notion of forcing and generic sets. *Fundamenta Mathematicae*, 56:325–345.

———, and A. Levy (1963). Independence results in set theory by Cohen's method II (abstract). *Notices Amer. Math. Soc.*, 10:592.

Frege, G. (1893). *Grundgesetze der Arithmetik, Begriffsschriftlich Abgeleitet*, volume 1. Jena.

Gitik, M. (1980). All uncountable cardinals can be singular. *Israel J. Math.*, 35(1–2):61–88.

Gödel, K. (1938). The consistency of the axiom of choice and of the generalized continuum hypothesis. *Proc. Nat. Acad. Sci. U.S.A.*, 24:556–557.

——— (1939). The consistency of the axiom of choice and of the generalized continuum hypothesis. *Proc. Nat. Acad. Sci. U.S.A.*, 25:220–224.

——— (1940). *The Consistency of the Axiom of Choice and of the Generalized Continuum-Hypothesis with the Axioms of Set Theory*. Annals of Math. Stud. 3. Princeton University Press, Princeton.

Gries, David, and Fred B. Schneider (1994). *A Logical Approach to Discrete Math*. Springer-Verlag, New York.

——— and ——— (1995). Equational propositional logic. *Information Processing Lett.*, 53:145–152.

Hartogs, F. (1915). Über das Problem der Wohlordnung. *Math. Ann.*, 76:438–443.

Hermes, H. (1973). *Introduction to Mathematical Logic*. Springer-Verlag, New York.

Hilbert, D., and P. Bernays (1968). *Grundlagen der Mathematik I, II*. Springer-Verlag, New York.

Hinman, P. G. (1978). *Recursion-Theoretic Hierarchies*. Springer-Verlag, New York.

Jech, T. J. (1978a). About the axiom of choice. In Barwise (1978), Chapter B.2, pages 345–370.

——— (1978b). *Set Theory*. Academic Press, New York.

Kamke, E. (1950). *Theory of Sets*. Translated from the 2nd German edition by F. Bagemihl. Dover Publications, New York.

Kunen, Kenneth (1980). *Set Theory: An Introduction to Independence Proofs*. North-Holland, Amsterdam.

Levy, A. (1979). *Basic Set Theory*. Springer-Verlag, New York.

Manin, Yu. I. (1977). *A Course in Mathematical Logic*. Springer-Verlag, New York.

Mendelson, Elliott (1987). *Introduction to Mathematical Logic,* 3rd edition. Wadsworth & Brooks, Monterey, California.

Monk, J. D. (1969). *Introduction to Set Theory*. McGraw-Hill, New York.

Montague, R. (1955). Well-founded relations; generalizations of principles of induction and recursion (abstract). *Bull. Amer. Math. Soc.*, 61:442.

Pincus, D. (1974). Cardinal representatives. *Israel J. Math.*, 18:321–344.

Rasiowa, H., and R. Sikorski (1963). *The Mathematics of Metamathematics*. Państwowe Wydawnictwo Naukowe, Warszawa.

Schütte, K. (1977). *Proof Theory*. Springer-Verlag, New York.

Shoenfield, Joseph R. (1967). *Mathematical Logic*. Addison-Wesley, Reading, Massachusetts.

——— (1971). Unramified forcing. In Dana S. Scott, editor, *Axiomatic Set Theory*, Proc. Symp. Pure Math., pages 357–381.

——— (1978). Axioms of Set Theory. In Barwise (1978), Chapter B.1, pages 321–344.

Sierpiński, W. (1965). *Cardinal and Ordinal Numbers*. Warsaw.

Skolem, T. (1923). Einige Bemerkungen zur axiomatischen Begründung der Mengenlehre. In *Wiss. Vorträge gehalten auf dem 5. Kongress der skandinav. Mathematiker in Helsingförs, 1922*, pages 217–232.

Smullyan, Raymond, M. (1922). *Gödel's Incompleteness Theorems*. Oxford University Press, Oxford.

Tarski, A. L. (1955). General principles of induction and recursion (abstract); The notion of rank in axiomatic set theory and some of its applications (abstract). *Bull. Amer. Math. Soc.*, 61:442–443.

——— (1956). *Ordinal Algebras*. North-Holland, Amsterdam.

Tourlakis, G. (1984). *Computability*. Reston Publishing Company, Reston, Virginia.

——— (2000a). A basic formal equational predicate logic – part I. *BSL*, 29(1–2):43–56.

——— (2000b). A basic formal equational predicate logic – part II. *BSL*, 29(3):75–88.

——— (2001). On the soundness and completeness of equational predicate logics. *J. Computation and Logic*, 11(4):623–653.

Veblen, Oswald, and John Wesley Young (1916). *Projective Geometry*, volume I. Ginn and Company, Boston.

Whitehead, A. N., and B. Russell (1912). *Principia Mathematica*, volume 2. Cambridge Univ. Press, Cambridge.

Wilder, R. L. (1963). *Introduction to the Foundations of Mathematics*. Wiley, New York.

Zermelo, E. (1904). Beweis daß jede Menge wohlgeordnet werden kann. *Math. Ann.*, 59:514–516.

——— (1908). Untersuchungen über die Grundlagen der Mengenlehre I. *Math. Ann.*, 65:261–281.

——— (1909). Sur les ensembles finis et le principe de l'induction complète. *Acta Math.*, 32:185–193.

# List of Symbols

$[f(0), \dots, f(n-1)]$, 251
$\mathbb{A} \times \mathbb{B}$, 189
$\pi$ (first projection of pairing function), 186
$\delta$ (second projection of pairing function), 186
$\mathscr{A}^{\mathscr{M}}$, 79
$\Gamma + \mathscr{A}$, 49
$M_{\mathbb{P}}$ (*adjacency map* of $\mathbb{P}$), 269
$\aleph_\alpha$, 465
$\beth$, 516
$f(n) = O(g(n))$ ("big-O" notation), 283
$(\exists a \in M) \dots$, 63
$\mathscr{A}(y_1, \dots, y_k])$, 20
$\mathscr{A}[y_1, \dots, y_k]$, 20
$\mathfrak{m}$, 458
$\mathfrak{a} \cdot_c \mathfrak{b}$, 472
$\mathrm{Card}(\prod_{i \in I} \mathfrak{k}_i)$, 485
$\mathfrak{a}^+$, 465
$\sum_{i \in I} \mathfrak{k}_i$, 484
$\kappa$, 458
$\mathrm{Card}(x)$, 458
$\mathrm{Cl}(R)$, 495
$r_{\mathbb{A}}(\mathbb{P})$ (*reflexive closure* of $\mathbb{P} : \mathbb{A} \to \mathbb{A}$), 262
$s(\mathbb{P})$ (*symmetric closure* of $\mathbb{P}$), 262
$t(\mathbb{P})$ (*transitive closure* of $\mathbb{P}$), 262
$\mathbb{P}^+$ (*transitive closure* of $\mathbb{P}$ (alternate notation)), 232, 262
$\mathbb{P}^*$ (*reflexive-transitive closure* of $\mathbb{P}$), 269
Cn, 458
$\mathrm{cf}(\alpha)$, 478
$\mathbb{P} \circ \mathbb{S}$ (*relational composition*), 253
$f * g$, 252
$a^{\mathscr{I}}$, 54
$\mathbf{D}(X)$ (set of sets definable from $X$), 223
$\mathbb{S}\langle a \rangle \downarrow$ ($\mathbb{S}$ is defined at $a$), 198
$\Delta_0$, 101, 380
$\boldsymbol{\Delta}_{\mathbb{A}} : \mathbb{A} \to \mathbb{A}$ (*diagonal relation on* $\mathbb{A}$), 257
$-$, 141
$<_\Sigma$, 413
$X \dotplus Y$, 412
$<_*$, 413
dom (*domain of a relation*), 195
$\emptyset$, 111, 131
$A \sim B$, 431
$A \not\sim B$, 431
$\Vdash^w$, 530
$\Vdash$, 536
$\models_{\mathfrak{I}}$, 80

$f : A \to B$, 26

$f^{\mathscr{I}}$, 54

glb($\mathbb{B}$), 347

$\mathbf{1}_{\mathbb{A}} : \mathbb{A} \to \mathbb{A}$ (*identity relation on* $\mathbb{A}$), 257

$\mathbb{S}[\mathbb{X}]$ (*image* of $\mathbb{X}$ under $\mathbb{S}$), 196

$\mathbb{S}^{-1}[\mathbb{X}]$ (*inverse image* of $\mathbb{X}$ under $\mathbb{S}$), 196

$\mathbb{S}\langle c\rangle$, 196

$\bar{i}$, 55

$p \perp q$, 520

inf($\mathbb{B}$), 67, 347

$b\,\mathbb{T}\,a$ ($\mathbb{T}$ *a relation*; it means $\langle a, b\rangle \in \mathbb{T}$), 194

$\mathbb{Z}$, 113

$\bigcap_{i=1}^{n} \mathbb{A}_i$, 142

$\bigcap_{1\leq i\leq n} \mathbb{A}_i$, 142

$\bigcap_{a\in\mathbb{I}} \mathbb{A}_a$, 193

$\cap$, 141

$\bigcap \mathbb{A}$ (*intersection of a class* $\mathbb{A}$), 153

$\mathbb{Z}$, 15

$(\iota z)\mathscr{Q}$, 74

$\kappa$-a.c., 553

$\kappa$-c.c., 553

Lim $(\alpha)$, 342

$\mathbb{L}$, 397

$L(\mathfrak{M})$, 55

$\mathbb{L}_N$, 397

$\lambda$ (used in $\lambda$-notation), 202

$\mapsto$ (alternative to $\lambda$-notation), 203

$\overline{\Gamma}$, 438

$\Gamma^{\infty}$, 438

$<$, 336

$\mathbb{L}_M$ (the *constructible universe*), 284

$\Lambda$, 35

$\Lambda$, 39

lub($\mathbb{B}$), 346

$\alpha - 1$, 342

$\mathbb{N}$, 12

$\langle \vec{x}_n \rangle$, 185

$\langle x_1, \ldots, x_n \rangle$ (*n-vector* or *n-tuple*), 185

$\langle \vec{x} \rangle$, 185

$\mathbb{N}$, 15

$\mathbb{N}$, 112, 233

$\omega$, 112, 234

$n, m, l, i, j, k$ (natural number variables), 235

$\not\models$, 61

$\nvdash$, 61

$\notin$, 116

$\widetilde{n}$, 88

On, 332

$OP$, 188

$<$ (abstract symbol for *order*), 284

Ord, 331

ord$(x)$, 397

$\triangleleft$, 374

$\cong$, 317

$\leq$ (abstract symbol for *reflexive order*), 285

$\bigcup_{\beta\in\alpha}(\{\beta\} \times X_\beta)$, 135, 412

$\alpha^{\cdot\beta}$, 423

$\alpha + 1$, 340

$\langle a, b\rangle$ (*ordered pair*), 186

$(\mathbb{A}, <)$, 286

$\prec$, 462

$\prec$ (a fixed order of logical and nonlogical symbols), 222, 223

$\preccurlyeq$, 461

$pr$ (the *predecessor* function on $\omega$), 239

$P^{\mathscr{I}}$, 54

$\mathbb{A}^n$, 192

$\mathbb{A}_1 \times \cdots \times \mathbb{A}_n$, 192

$\mathbb{P}^0$ (0*th power of a relation*), 257

$\mathbb{P}^n$ (*positive power of a relation*), 256

$\prod_{a\in I}\mathbb{F}_a$, 207
$\times_{i=1}^{n}\mathbb{A}_i$, 192
$\times_{1\le i\le n}\mathbb{A}_i$, 192
${}^{I}A$, 208
$\exists!$, 67
$A/P$, 277
$R_N(\alpha)$, 359
ran (*range of a relation*), 195
$\rho$, 369
$rk$, 369
$\mathbb{Q}$, 113
$\mathbb{Q}$, 15
$\mathbb{R}$, 15
$\mathbb{R}$, 113
$\mathbb{S}^{-1}$ (*inverse* of $\mathbb{S}$), 196
$\restriction$, 55
$\mathbb{T}\restriction\mathbb{A}$ (restrict *inputs* of $\mathbb{T}$ to be in $\mathbb{A}$), 198
$\mathbb{T}\upharpoonleft\mathbb{A}$ (alternate notation for "$\restriction$"), 199
$\mathbb{T}\mid\mathbb{A}$ (that is, $\mathbb{T}\cap\mathbb{A}^2$), 198
$S(x)$, 340
string
  $\lambda$, 13
  $\equiv$, 13
$\subseteq$, 117, 139
$\nsubseteq$, 117
$\supseteq$, 117, 139
$\nsupseteq$, 117
$\subset$, 119, 139
$\subsetneq$, 119
$\subsetneqq$, 119
$\supset$, 139
$n+1$ (the *successor* of $n\in\omega$, i.e., $n\cup\{n\}$), 242
$\mathfrak{a}+_c\mathfrak{b}$, 470
$sp$, 309
sup($\mathbb{B}$), 346
sup$^+(A)$, 347
$t^{\mathscr{M}}$, 79
**Term**($\mathfrak{M}$), 55
$S^+$ (the set of all nonempty strings over the set $S$), 224
$TC(\mathbb{A})$ (*transitive closure* of the class $\mathbb{A}$), 265
$\lhd$ (order of "definable sets"), 219, 223, 225
$\langle\ldots\rangle$, 20
$\mathbb{U}_M$, 144
$\mathbb{U}_N$ (the class of all sets and atoms), 144
$\mathbb{U}$, 144
$\mathbb{S}\langle a\rangle\uparrow$ ($\mathbb{S}$ is undefined at $a$), 198
$\bigcup_{i=1}^{n}\mathbb{A}_i$, 142
$\bigcup_{1\le i\le n}\mathbb{A}_i$, 142
$\bigcup_{a\in\mathbb{I}}\mathbb{A}_a$, 193
$\cup$, 141
$\bigcup\mathbb{A}$ (*union of a class* $\mathbb{A}$), 150
$\bigcup A$ (*union of a set* $A$), 152
$U(x)$ ("$x$ is an urelement"), 114
$V_N(\alpha)$, 359
$\boldsymbol{V}=\boldsymbol{L}$, 408
$\mathbb{V}=\mathbb{L}$, 408
$\vec{a}_n$, 21
$\vec{a}$, 21
$\vec{x}_n$, 34
$\mathbb{V}_M$, 144
$\mathbb{V}_N$ (*the class of all sets*), 145
$\mathbb{V}$, 145
$\mathbf{WF}_N$, 359
**Wff**($\mathfrak{M}$), 55
ZF, 108, 228
ZFC, 2, 108, 229

# Index

- absolute formula, 382
- absolute term, 382
- absolutely provable, 38
- absoluteness of rank, 394
- AC, 215, 274
  - global, 226
  - strong, 226
- Aczel, P., 498
- addition, 246
  - over $\omega$, 246
    - is associative, 248
    - is commutative, 247
- adjacency map, 269
- adjacency matrix, 269
- ∀-introduction, 44
- alephs, 465
- algebraic topology, 275
- algorithm, 283
- alphabet, 7, 13
- ambiguity, 25
- ambiguous, 25, 498
- antichain, 520
- antinomies, 104
- Apostol, T., 228
- *argot*, 40
- arithmetization, 90
- arity, 9
- array, 233
- ascending sequence, 348
- associativity, 17, 256
- at most enumerable, 442
- atom, *see* urelement
- axiom, 8
  - comprehension, 121
  - logical, 8
  - nonlogical, 8, 37
    - of regularity, 159
    - urelements are atomic, 116
  - of (unordered) *pair*, 145, 211
  - of choice, *see* AC
  - of collection, 163, 204
  - of constructibility, 408
  - of dependent choices, 298
  - of foundation, 158
  - of infinity, 234
  - of power set, 180
  - of replacement, 161, 163, 371
  - of union, 151
  - special, 8
- axiomatic theories, 39
- axiomatized, 39
- axioms, logical, 35

- Barwise, J., 192, 368, 395
- basic language, 108
- Bernays, P., 34, 42, 315
- Berry's paradox, 104
- beth, 516
- bijection, *see* 1-1 correspondence
- binary digit, 455
- binary notation, 455
- binary relation, *see* relation
- bit, 455
- Blum, E., 228
- Blum's speedup theorem, 228
- BNF, 18
- Boolean, 9
- Boolean addition, 270
- Boolean sum, 271
- bound variable, 19
- Bourbaki, N., 5, 43, 229
- Brouwer, L. E. J., 4, 12
- Burali-Forti, C., 122

- calculational proof, 85
- Cantor, G., 105, 122

cardinal, 207, 458, 467
  inaccessible, 483
  strongly inaccessible, 483
  weakly inaccessible, 483
cardinal multiplication, 472
cardinal number, 431, 458, 467
cardinal product, 472
cardinal successor, 465
cardinality, 431, 458, 467
cardinals
  product of family, 485
  sum of, 470
  sum of family, 484
Cartesian product, 189
  of many classes, 192
category theory, 275
c.c.c., 553
CH, 466
chain, 354, 520
choice function, 216
class, 136
  $\in$-closed, 237
  domain of, 195
  $f$-closed, 434
  proper, 137
  $R$-closed, 495
  range of, 195
  transitive, 236
class term, 134
closed formula, 20
closed term, 20
closed under, 21, 434
closure, 21
  *see also* relation
cofinal subsets, 478
cofinality, 478
Cohen, P. J., 229, 467, 487, 526
Cohen extension, 524, 526
Cohen generic real, 553
collapsing cardinals, 551
collapsing function, 310
collection, 149
collection axiom, *see* axiom
commutative diagram, 275
compactness theorem, 65
comparable, 520
compatible, 520
complement, 145
complete, 97
complete arithmetic, 40
complete lattice, 349
completeness, 6
completeness theorem, 54, 64, 65, 97
completion, 97
composition, 195
  *see also* relation
computer programming, 232
concatenation, 13, 252
conditions, 520
congruence, 261
conjunction, 17
conjunctionally, 85
connectives, 9
conservative, 68, 74
conservative extension, 72, 168
consistency, 61, 531
consistency theorem, 64, 65
constant, 10
  imported, 55
constructible object, 397
constructible sets, 396
constructible universe, 219, 229, 284, 395
*construction formative*, 43
continuum hypothesis, 3, 466
correct, 88
correct theory, 88
countable, 64, 90, 314, 442
countable chain condition, 553
course-of-values induction, 281, 294
CTM, 314
cumulative hierarchy, 359

De Morgan's laws
  for classes, 154
  generalized, 212
decision problem, 41
Dedekind, R., 449
Dedekind finite, 449
Dedekind infinite, 449
deduce, 38
deduction theorem, 49
deductions, 1
definability, 61, 62
  in a structure, 61
definition by recursion, 26
$\Delta_0$-formulas, 380
$\Delta$-system, 555
  root of, 555
dense, 520
dense below, 559
denumerable, 442
derivation, 22
derived rule, 37, 39, 41
Devlin, K. J., 229
diagonalization, 121, 156
difference, 250
  of two classes, 141
  over $\omega$, 250
disjoint classes, 141
disjoint union, 412
distributive laws, 95, 212
  for $\omega$, 282
  for $\times$, 213
  generalized, 212

domain, 54
double induction, 248, 300
dummy renaming, 46

∃-introduction, 37
elimination of defined symbols, 69, 71
embedding, 318
empty set, 100, 111, 131
*Entscheidungsproblem*, 41
enumerable, 442
$\varepsilon$-numbers, 426
$\varepsilon$-term, 76
equinumerous, 431
equipotent, 431
equivalence class, 276, 277
equivalence relation, 276
equivalence theorem, 52
existential formula, 67
explicit listing, 147
expression, 2, 8, 13
extension, 7, 194
  Cohen, 524
  generic, 524
  of a condition, 520
extensional, 31, 312
extensionality, 67

family
    of sets, 150
    indexed, 206
    intersection of, 153
    union of, 150
    quasi-disjoint, 555
Feferman, S., 228, 447, 530
filter, 521
  generated by a chain, 522
finitary, 4
finitary rule, 503
finite, 389
finite sequence, 251
  length of, 251
finitely satisfiable, 98
first incompleteness theorem, 87
first order definable, 111
fixed point, 351, 438
fixpoint, 351, 438
forcing, 315
forcing conditions, 520
forcing language, 528
formal interpretation, 78
  of a theory, 83
formal isomorphism, 84
formal language, 111, 115
  first order, 7
formal model
  of a theory, 83
formal natural numbers, *see* set
formalize, 6
formalized, 3
formula
  absolute, 382
  mixed-mode, 62
  prime, 29
  propositional, 29
  satisfiable, 31
  tautology, 31
  unsatisfiable, 31
formula form, 35
formula schema, 35
foundation axiom, 102
Fraenkel, A. A., 105
free for, 33
free variable, 19
Frege, G., 121
function, 199
  bijective, 204
  collapsing, 310
  continuous, 348
  countably continuous, 348
  diagram, 275
    commutative, 275
  expansive, 353
  inclusive, 353
  increasing, 348
  injective, 203
  inverse of, 273
  left inverse of, 272
  left-invertible, 274
  monotone, 348
  non-decreasing, 348
  one-to-one, 203
  order-preserving, 317
  partial, 199
  right inverse of, 272
  right-invertible, 274
  surjective, 204
function diagram, 275
function substitution, 201

$G$-interpretation, 525
$\Gamma$-closed, 437
$\Gamma$-induction, 438
GCH, 466, 484
generalization, 45, 120
generalized continuum hypothesis, 408, 466, 484
generic, 518
generic extension, 524, 526
global choice, *see* AC
Gödel, K., 3, 6, 229, 395, 467
Gödel operations, 396
Gödel-Rosser incompleteness theorem, 92
Gödel's second incompleteness theorem, 93

Gries, D., 5
ground model, 518, 526

Hausdorff, F., 230
Hausdorff's theorem, 230, 357
Hermes, H., 43
Heyting, A., 4
Hilbert, D., 4, 12, 42, 93, 315
Hinman, P. G., 498
hypersets, 156, 368

IC, 293
iff, 13
I.H., 23
image, 177
image of a class under a relation, 196
immediate predecessor set, 497
immediate predecessors, 25, 497
implied multiplication, 260
imported constant, 55
inaccessible, 483
incompatible, 520
incompletable, 89
incompletableness, 62, 87
incompleteness, 6
incompleteness theorem (first, of Gödel), 112
indefinite article, 75
index class, 193
indexed family of sets, *see* family of sets
individual variables, 9
induced order, 319
induction, 235
  on finite sets, 441
  on *TC*, 393
  on WR-finite sets, 441
  over $\overline{\Gamma}$, 438
  over $\delta$, 343
  over On, 343, 344
  over $\omega$, 235
    course-of-values, 281
induction hypothesis, 23, 235
inductive definitions, 19, 21, *see also* recursive definitions
inductive set, *see* set
inductiveness condition, 293
infima, 347
infimum, 347
infinite descending chain, 297
infix, 14, 195
informal, 10
initial ordinals, 459
injection, *see* function, injective
injective function, *see* function
input object, 193
instance, 37, 129
interpretation, 54
interpretation function, 525
intersection, 153
  of a class, 153
  of a family of sets, 153
  of a higher order collection, 193
  of many classes, 142
  of two classes, 141
inverse image of a class under a relation, 196
iota notation, 73
i.p., 25, 497
i.p.s., 497
irreflexive, 284
isomorphic, 240
isomorphic image, 242
isomorphism, 241, 313, 316
iteratively, 22

Jech, T. J., 229, 395

Kamke, E., 355
$\kappa$-antichain condition, 553
$\kappa$-chain condition, 553
KP, 192
KPU, 192
Kronecker, L., 5
Kuratowski-Zorn theorem, 230, 356

$\lambda$-notation, 202
language
  countable, 64
  extension, 55
  first order, 16
  restriction, 55
  uncountable, 64
lattice, 521
laws of exponents, *see* relation, positive power of
$\in$-least, 244
least number principle, 281
left inverse, *see* function
Leibniz, G. W., 35
Leibniz rule, 52
Levy, A., 199, 228, 439, 447, 467
lexicographically, 91, 413
limit cardinal, 465, 555
limit ordinal, 342
Lindemann, F., 5
linear order, *see* order
linearly ordered class, 287
linearly ordered set, 230, 287
LO class, *see* linearly ordered class
LO set, *see* linearly ordered set
logical symbols, 9
logically implies, 54
Löwenheim, L., 64
lower bound, greatest, 347

$\mathfrak{m}$-based rule class, 503
$M$-generic sets, 522
$\mathfrak{M}$-instance, 56
$\mathfrak{M}$-term, 55
$\mathfrak{M}$-formula, 55
Mal′cev, A. I., 65
Manin, Yu. I., 40
material implication, 17
mathematical theory, *see* theory
matrix multiplication, 283
maximal element, 287
maximum element, 287
MC, 289
  weak, 372
metalanguage, 7
metamathematics, 7
metatheorems, 11
metatheory, 4, 7
metavariable, 169
minimal condition, 289
minimal element, 287
$\in$-minimal element, 239
minimality principle, 239
$\in$-minimum, 244
minimum element, 287
model, 57
  countable, 64
  uncountable, 64
modus ponens, 37, 120
monotonicity, 51, 531
Montague, R., 306
Moschovakis, Y. N., 186, 502
Moss, L., 368
Mostowski, A., 310, 426
MP, 37
multiplication of natural numbers, 259, 282
  is associative, 282
  is commutative, 282

natural numbers, 12, 235
  distributive law, 282
natural projection, 280
non-deterministic, 498
non-extensional, 312
non-null, 141
non-void, 141
non-monomorphic, 498
normal, 349
notion of forcing, 520
null, 141
numeral, 42, 88
$n$-vector, 185

object variables, 9
occurrence, 13
occurs in, 13
1-1 correspondence, 64, 204, 273
1-1 function, *see* function
one point rule, 71, 201
one-to-one function, *see* function
onto, 64
open, 520
operator, 437
  inductive, 438
  monotone, 437
order, 284
  lexicographic, 224
  linear, 287
  partial, 284
  total, 287
order of $x$, 397
order-preserving, 348
order type, 241, 339
order-isomorphic, 317
order isomorphism, 317
ordered disjoint sum, 412
ordered $n$-tuple, 185
ordered pair, 184, 188
ordered sequence, 20
ordinal, 324, 331
  cofinal in, 478
  limit, 342
  of a monotone operator, 503
  regular, 479
  singular, 479
  successor, 342
ordinal exponentiation, 423
ordinal number, 43, 324, 331
ordinals, 65, 219, 284, 324
ordinary recursion theory, 196
output object, 193

pairing function, 184, 186
  first projection of, 186
  second projection of, 186
pairwise disjoint, 216
pairwise disjoint sets or classes, 153
paradoxes, 104
parameter, 170, 137, 194
parsable, 30
parse, 22
partial function, *see* function
partial multiple-valued function, 199
partial order, *see* order
partially ordered class, 286
partially ordered set, 286
partition, 278
Peano arithmetic, 87, 101
pigeon-hole principle, 432
Pincus, D., 468
Platonist, 103

PO class, *see* partially ordered class
PO set, *see* partially ordered set
Post, E., 97
Post's theorem, 97
power class, 178
power set, 149, 178
predecessor, 238, 498
predicate, 10
  defined
    subset, *see* subset relation
prefix, 13, 195
preservation of cardinals, 555
prime factorization theorem, 446
primitive recursive pairing function, 189
principle 3 of set construction, 161
priority, 17, 533
    of set operations, 154
product, 485
programming formalism, 233
programming language, 233
proof, 1, 38
    $\Gamma$-, 38
    by auxiliary constant, 53
    by cases, 52
    by contradiction, 51
proper class, *see* class
proper extension, 520
proper prefix, 13
proper subset, *see* subset relation
propositional axioms, 97
propositional calculus, 97
propositional connectives, 9
propositional logic, 97
propositional segment, 97
propositional valuations, 30
propositional variable, 29
provably equivalent, 43
proved from, 38
pure recursion, 308
    over $\delta$, 344
    over On, 344
pure sets, 310, 346
pure theory, 57

quantifier
  bounded, 149
quotient set, 277

rank, 369
Rasiowa, H., 42
$\mathscr{R}$-closed, 21
"real sets", 110
recursion, 20
    over $\delta$, 344
    over On, 343
recursive, 89
recursive definitions, 21, 244, 301
  over $\omega$, 244
recursively axiomatizable, 40
recursively axiomatized, 39
reference set, 145
reflection principle, 504
reflexive closure, 262
reflexive-transitive closure, 362
regularity axiom, *see* axiom, nonlogical
relation, *see* predicate, 20, 194
  antisymmetric, 260
  binary, 194
  closure, 262, 495
    reflexive, 262
    symmetric, 262
    transitive, 262
  composition, 253
  converse of, 196
  defining formula of, 194
  diagonal, 257
  domain of, 195
  equivalence, 276
  extension of, 198
  field of, 195
  identity, 257
  input of, 195
  inverse of, 196
  irreflexive, 260
  left field of, 196
  left-narrow, 301
  $n$-ary, 194
  nontotal, 196
  onto, 196
  output of, 195
  positive power of, 256
    laws of exponents, 259
  range of, 195
  reflexive, 260
  restriction of, 198
  right field of, 196
  setlike, 301
  single-valued, 199
  symmetric, 260
  total, 196
  transitive, 260
  unary, 194
  well-founded, 297
relational composition, *see* relation, composition
relational extension of a formula, 194
relational implementation, 194
relative consistency of ZFC$-$f, 367
relative universe, 145
relativization, 79
replacement axiom, *see* axiom

reverse inclusion, 521, 549
right inverse, *see* function
$R$-induction, 496
Rosser, J. B., 92
rule, 495
  finitary, 495
  infinitary, 495
rule set, 494
rules of inference, 8, 29
Russell, B., 74, 104, 122, 439

satisfiable, 57
  finitely, 57
schema, 35
schema instance, 35
Schneider, F. B., 5
scope, 15, 17, 533
segment, 230, 301
  closed, 301
  initial, 301
selection axiom, 229
self-reference, 94
semantics, 6
sentence, 20
separation, 67
sequence, 208
set, 99
  $\in$-closed, 237
  countable, 442
  Dedekind finite, 449
  Dedekind infinite, 449
  definable, 219, 220, 223
  empty, 111
  enumerable, 442
  finite, 431
  inductive, 233
  inductively defined, 495
  infinite, 431
  name, 110
  of (formal) natural numbers, 234
  of natural numbers, 112
  pure, 310
  rank of, 206
  recursively defined, 495
  successor, 233
  transitive, 220, 236, 331
  uncountable, 442
  well-founded, 158, 359
  WR-finite, 440
  WR-infinite, 440
sethood, 18, 106
set term, 126
    by listing, 133
set universe, 144
Shoenfield, J. R., 395
Sikorski, R., 42
simple completeness, 63
simply complete, 88
simultaneous substitution, 34
singleton, 147, 162
size limitation doctrine, 161
Skolem, T., 64
Skolem function, 76
Skolem paradox, 508
$\in$-smallest, 244
Smullyan, R., 88
sort, 17
soundness, 59, 81
specialization, 44, 117
stage, 24
  of collecting type, 219
  of powering type, 219
  of set formation, formal definition, 368
  principle 0 of set construction, 102
  principle 1 of set construction, 102
  principle 2 of set construction, 102
string, 13
  empty, 13
  $\lambda$, 13
  equality, 13
  $\equiv$, 13
  prefix, 13
    proper, 13
strong choice, *see* AC
strong limit, 483
strongly inaccessible, 483
structure, 54
  domain of, 54
  expansion of, 55, 72
  reduct of, 55
  underlying set of, 54
  universe of, 54
subclass, 139
  proper, 139
subscripted variable, 233
$\subseteq$, 21
subset relation, 117, 139
  proper, 119
substitutable for, 33
substitution, 32
  simultaneous, 34
substitution axiom, 35
substring, 11, 13
subtraction, *see* difference
successor cardinal, 465, 555
successor ordinal, 342
superclass, 139
  proper, 139
superset relation, 117
support, 309
support function, 346

supremum, 346
surjection, *see* function, surjective
surjective function, *see* function
symbol sequence, 2
symmetric closure, 262
syntactic variable, 169

table, 20
Tarski, A. L., 306, 530
Tarski semantics, 87
$\tau$-term, 76
tautologies, 29
tautology theorem, 97
term, 126
  absolute, 382
theorem, 37
  $\Gamma$-, 37
theorem schema, 41
theory, 39
  absolute, 40
  applied, 40
  complete, 88
  conservative extension of, 47
  consistent, 39, 229
  contradictory, 39
  correct, 88
  extension of, 47
  first order, 39
  formal interpretation of, 83
  formal model of, 83
  incompletable, 228
  incomplete, 88
  inconsistent, 39
  $\omega$-consistent, 88
  pure, 40
  semantically complete, 63
  simply complete, 88
  simply incomplete, 88
  sound, 57
total, 186
total function, 143
total order, *see* order
totally defined function, 143
totally ordered set, 230
Tourlakis, G., 228
transfinite, 284
  construction, 284
    sequence, 348
transitive, 284
transitive class, *see* class
transitive closure, 232, 262
  of a class, 265
transitive set, *see* set
transitivity of $\vdash$, 38
transpose, 271
trichotomy, 241, 243, 245, 281, 287
true, 110
truth (value) assignment, 30
truth functions, 31
type, 17

unambiguous, 26, 55, 498
unary, 18
unbounded, 479
uncountable, 64, 90, 442
undecidable sentence, 88
underlying set, 54
union, 24, 150, 152
  of a class, 150
  of a family of sets, 150
  of a higher order collection, 193
  of many classes, 142
  of two classes, 141
uniquely readable, 30
universal closure, 45
universal quantifier, 17
universe, 144
unordered pair, 147
upper bound, 346
  least, 346
urelement, 99, 114
*Urelemente*, 100

vacuously satisfied, 32
valid, 57
  logically, 57
  universally, 57
valuation, 30, 98
variable
  bound, 19
  free, 19
  frozen, 50
variant, 36, 46
Veblen, O., 53
vector, 185
vector notation, 21
void, 141
von Neumann, J., 104
von Neumann universe, 107

Warshall, S., 283
weak equality, 202, 279
weak forcing, 530
weak MC, 372
weakly continuous, 349
weakly inaccessible, 483
weakly normal, 349
well-defined, 280
well-founded relations, 297
well-founded sets, 158, 359

well-ordering, 219, 223, 284, 289
Whitehead, A. N., 74, 439
Wilder, R. L., 449, 455, 458
WO class, 289
WR-finite, 440
WR-infinite, 440

Young, J. W., 53

Zermelo, E., 105, 230, 355
Zermelo's well-ordering principle, 355
Zermelo's well-ordering theorem, 230
Zermelo-Fraenkel axioms, 108
Zermelo-Fraenkel set theory, 228
*Ziffern*, 42
Zorn's lemma, *see* Kuratowski-Zorn theorem